2009-09

Control Based Mobile Ad Hoc Networking for survivable, dynamic, mobile Special Operation Force communicati

Masacioglu, Mustafa.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CONTROL BASED MOBILE AD HOC NETWORKING FOR SURVIVABLE, DYNAMIC, MOBILE SPECIAL OPERATION FORCE COMMUNICATIONS

by

Marlon McBride
Mustafa Masacioglu

September 2009

Thesis Advisor: Alex Bordetsky
Second Reader: Michael Clement

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Control Based Mobile Ad Hoc Networking for Survivable, Dynamic, Mobile Special Operation Force Communications		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Marlon McBride, Mustafa Masacioglu			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic mobile communication for tactical Special Operation Force (SOF) networks, as well as SOF units that are ad hoc networking with first responders conducting emergency/rescue and disaster relief operations. Such network scenarios cannot rely on centralized and organized connectivity, and should instead employ applications of newly developing Control Based Mobile Ad Hoc Networking (CBMANET). In a CBMANET environment, an autonomous collection of mobile users communicate over relatively bandwidth constrained wireless links by taking benefit of nodes mobility and topology control in combination with mobile platform switching. The network is decentralized. All network activity, including discovering the topology and delivering messages, must be executed by the nodes themselves (i.e., routing functionality will be incorporated into mobile nodes).

Harnessing the tremendous flexibility and efficiency of CBMANET would allow for better control and protection of ad hoc mobile networks. Therefore, we need to work tirelessly to improve our capabilities in the three aforementioned control spaces.

14. SUBJECT TERMS Control Based Mobile Ad Hoc Networking, CBMANET, MANET, Routing Protocol, Wireless Network			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CONTROL BASED MOBILE AD HOC NETWORKING FOR SURVIVABLE, DYNAMIC, MOBILE SPECIAL OPERATION FORCE COMMUNICATIONS

Marlon McBride
Major, United States Army
B.S., Jackson State University, 1996

Mustafa Masacioglu
Captain, Turkish Army
B.S., Turkish Military Academy, Ankara, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Authors: Marlon McBride

Mustafa Masacioglu

Approved by: Alex Bordetsky
Thesis Advisor

Michael Clement
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic mobile communication for tactical Special Operation Force (SOF) networks, as well as SOF units that are ad hoc networking with first responders conducting emergency/rescue and disaster relief operations. Such network scenarios cannot rely on centralized and organized connectivity, and should instead employ applications of newly developing Control Based Mobile Ad Hoc Networking (CBMANET). In a CBMANET environment, an autonomous collection of mobile users communicate over relatively bandwidth constrained wireless links by taking benefit of nodes mobility and topology control in combination with mobile platform switching. The network is decentralized. All network activity, including discovering the topology and delivering messages, must be executed by the nodes themselves (i.e., routing functionality will be incorporated into mobile nodes).

Harnessing the tremendous flexibility and efficiency of CBMANET would allow for better control and protection of ad hoc mobile networks. Therefore, we need to work tirelessly to improve our capabilities in the three aforementioned control spaces.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARMS	AERIAL RECONNAISSANCE MULTI-SENSOR
ARST	AERIAL RECONNAISSANCE SUPPORT TEAM
BWSR	BANDWIDTH SAVINGS RATION
CBMANET	CONTRAL BASED AD HOC NETWORKING
CENETIX	CENTER FOR NETWORK INNOVATION AND EXPERIMENTATION
C-IED	COUNTER IED
DARPA	DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
DOD	DEPARTMENT OF DEFENSE
DVOIP	DYNAMIC VOICE OVER IP
IED	IMPROVISED EXPLOSIVE DEVICE
ITMANET	INFORMATION THEORY FOR MOBILE AD HOC NETWORKS
JTRS	JOINT TACTICAL RADIO SYSTEM
MANET	MOBILE AD HOC NETWORK
MIMO	MULTIPLE INPUT MULTIPLE OUTPUT
NCW	NETWORK CENTRIC WARFARE
NOC	NETWORK OPERATION CENTER
ODIN	OBSERVE, DETECT, IDENTIFY, NEUTRALIZE
OFDM	ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING
PHY	PHYSICAL LAYER
PRNET	PACKET RADIO NETWORK
QOS	QUALITY OF SERVICE
QRF	QUICK RESPONSE FORCE
SAOFDM	SELF ALIGNING OFDM
SDR	SOFTWARE DEFINED RADIO
SOCOM	SPECIAL OPERATIONS COMMAND
SOF	SPECIAL OPERATION FORCES
SURAN	SURVIVABLE ADAPTIVE RADIO NETWORK
SYNAPSE	SYNTHESIZING ADAPTIVE PROTOCOLS BY SELECTIVE ENUMERATION

TNT	TACTICAL NETWORK TOPOLOGY
TOC	TACTICAL OPERATION CENTER
UAV	UNMANNED AERIAL VEHICLE
UWB	ULTRA WIDE BAND

ACKNOWLEDGMENTS

Mustafa Masacioglu:

This thesis is dedicated to my wonderful family. Throughout the entire process, my wife, Ozlem and my daughter, Kayra, provided me with enormous encouragement and unwavering support. Without my family's love, patience, and inspiration, this work would not have been possible. I thank you and love you both dearly.

I would like to thank our thesis advisor, Dr. Alex Bordetsky, for holding us to such a high standard of academic performance. Dr. Bordetsky, I truly thank you for your invaluable insight into our thesis topic. Without your guidance, our thesis would not have come to fruition. We know that you are a very busy man but you always made time to answer any and every question we may have had. Thank You!

I would like to thank our co-advisor, Mike Clement, for his willingness to assist us in our thesis. You never hesitated to provide your feedback to us and we could always count on a timely turn-around in drafts we sent to you. Your input definitely made our thesis better. Thanks for your commitment and the "red ink."

Finally, I would like to extend a special thanks to our DARPA family, Robert Henry and Tim Gibson. Thanks for allowing us to participate in your research and responding quickly to any information requests we sent to you. You do not know how much we appreciate your help. Thanks.

Bu çalışmamı, desteğini ve sevgisini biran olsun eksik etmeyen değerli eşim Özlem ve sevgisiyle bana hayat veren biricik kızım Kayra'ya adıyorum. Sizleri çok seviyorum.

Marlon McBride:

First things first, thank you Heavenly Father for making not only this thesis, but everything I've accomplished possible. You continuously prove that with You all things are possible.

To my beautiful wife, Kym, thank you for your unmatchable love and support. Thanks for the motivation during those times when I thought I could not go on. You have always had the perfect blend of love and drill sergeant like tendencies in you that helped me to make it to the next day. You helped me to keep it together and to finish the race. I Love You!

To my wonderful children, Marlon II, Christion, and Ambria, I love you with all of my heart. You may not have realized it but you are the reason I can keep my head up when going through the hard times. Just one look, one simple word, is enough to make me forget all the stresses and vicissitudes of life. Never forget that I sincerely love you!

I would like to thank our thesis advisor, Dr. Alex Bordetsky. Sir, thank you for your dedication to our project. You have to be one of the busiest men I know. I do not know how you did it but you always had time to make sure we were on the right track. Thanks for your guidance along the way and know that I will never forget the role you played in my NPS experience.

My second reader, Mike Clement, you are totally awesome! Words cannot express the level of gratitude I have for you. You provided timely and most importantly, critical feedback that made our thesis a lot better than it would have been had we not had it. Thanks for all that you have done.

Finally, a much deserved special thanks to my friends at DARPA, Robert "Bob" Henry and Tim Gibson. Gentlemen, thank you both so very much for all that you've done for us and our thesis. We realize you did not have to assist us at all but you chose to anyway. You do not know the magnitude of your efforts. Thanks and good luck in all your future endeavors.

I. INTRODUCTION

A. WIRELESS NETWORKS

By now, most people have either come into contact or are somewhat familiar with wireless networks. Mobile devices, such as Personal Digital Assistants (PDAs), cell phones, and smart phones can be found on everyone from small children to the most senior of senior citizens. Wireless networks have penetrated their way into almost every aspect of our lives. With the constant demand for bigger, better, and faster, they will no doubt continue to push the boundaries of our imagination and capabilities. As the popularity of wireless networks and mobile devices has grown, so has the desire for research in the area of Mobile Ad Hoc Networks (MANETs).

Since the mid 1990s, significant work has been done in the area of MANETs, and we can expect more in future years. In fact, the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE) have worked vigorously to standardize routing and medium access protocols. Because MANETs present enormous promise when societies are faced with emergencies like natural disasters, military conflicts, and emergency medical situations, these organizations, as well as many others, recognize the tremendous value they bring to the table.

B. MANET DEFINITION

For the purpose of this thesis, a MANET is a self-configuring network where every device connected to it serves as a router devoid of any centralized structure. Mobile implies that these networks are highly flexible and adaptable, and they can be stood up at a moment's notice. Ad Hoc originates from the Latin language and means "for this," or "for this only" [1]. This implies that these networks are created with a specific purpose in mind. There are three categories of ad hoc networks: first generation, second generation, and third generation.

C. CHARACTERISTICS OF MANETS

In [2], MANETs consist of mobile platforms (nodes), which are free to move about the coverage area. These nodes may be mounted in or on any type of vehicle, including people. MANETs can operate as a stand-alone system or can connect to a fixed network. When attached to a fixed network, a MANET is expected to operate as a "stub" network connecting to a fixed internetwork. Stub networks will allow traffic generated from and destined to internal nodes, but will not allow outside users to initiate traffic. As you might assume, MANET nodes are equipped with some type of wireless transmitter and receiver. These antennas may be omni-directional, point-to-point, or some combination thereof.

D. COMPARISON OF MANETS AND STRUCTURED NETWORKS

In [2], Corson and Macker give us several distinct differences between MANETs and structured networks:

1. Dynamic Topologies

Nodes are free to move arbitrarily; thus, the network topology, which is typically multi hop, may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

2. Bandwidth-Constrained, Variable Capacity Links

Wireless links will continue to have significantly lower capacity than their hardwired counterparts do. In addition, the realized throughput of wireless communications—after accounting for the effects of multiple access, fading, noise, and interference conditions, is often much less than a radio's maximum transmission rate. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e., aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands

will continue to increase as multimedia computing and collaborative networking applications multiply, thereby putting more demand on an already strained network.

3. Energy-Constrained Operation

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. Current technologies were not designed with MANETs in mind. These technologies tend to consume large amounts of power, which could limit the use of some mobile devices.

4. Limited Physical Security

Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure in more centralized approaches.

E. HISTORY OF MOBILE AD HOC NETWORKS

1. First Generation Ad Hoc Networks

First generation ad-hoc networks were originally called “packet radio networks” (PRNET) and were sponsored by the Defense Advanced Research Projects Agency (DARPA) beginning in the early 1970s. The need to provide both computer network access to mobile hosts and terminals and computer communications in a mobile environment motivated this research. The PRNET provided, via a common radio channel, the exchange of data between geographically separated computers. One of the benefits was mobility; a packet

radio (PR) could operate while in motion. Second, since there were no wires to run, the network could be installed or deployed quickly. A third advantage was the ease of reconfiguration and redeployment. The PRNET protocols took advantage of broadcasting and common-channel properties to allow expansion and contraction automatically and dynamically. A group of packet radios leaving the original area simply departed, with no adverse affect on the rest of the network. Having left the network, it had the flexibility to function as an autonomous group, rejoin the original network, or join another group. The PRNET featured fully automated network management. It self configures upon network initialization, reconfigures upon gain or loss of packet radios, and has dynamic routing. In [3], the PRNET system is comprised of the following:

- The PRNET subnet, with its packet radios. The PRNET subnet provides the means of interconnecting a community of users.
- The collection of devices (host computers and terminals), each attached to a packet radio via a High-Level Data Link Control (HDLC) interface that wished to exchange data in real time.

2. Second Generation Ad Hoc Networks

In the 1980s, the PRNET program evolved into the second generation of ad hoc networks known as the Survivable Adaptive Radio Network (SURAN). The SURAN program provided a packet-switched network to the mobile battlefield in an environment without an existing infrastructure. The SURAN Program was established to research and identify solutions for making radios smaller, less expensive, and less vulnerable to electronic attacks.. Because of the demonstrated advantages of PR networking for the battlefield environment, SURAN used PR as its means to evaluate and demonstrate an integrated network based on its technology. The overall approach taken during the SURAN Program can be divided into three main efforts [4]:

- Develop theoretically founded, survivable and adaptive network algorithms, particularly for, but not limited to, the broadcast radio environment, that are capable of effectively supporting continued

operation in large, dynamic networks (with thousands of nodes) despite sophisticated attempts to disrupt communication.

- Develop an experimental PR network that both integrates and demonstrates SURAN network algorithms and facilitates technology transfer of an experimental SURAN network to potential users.
- Develop automated evaluation tools both for simulating the network protocols on a computer and for testing the experimental PR network in the laboratory using an RF environment emulator to control the network connectivity. Evaluate and demonstrate the performance and vulnerabilities of the experimental network and use the identified deficiencies to help direct the algorithm and network development efforts.

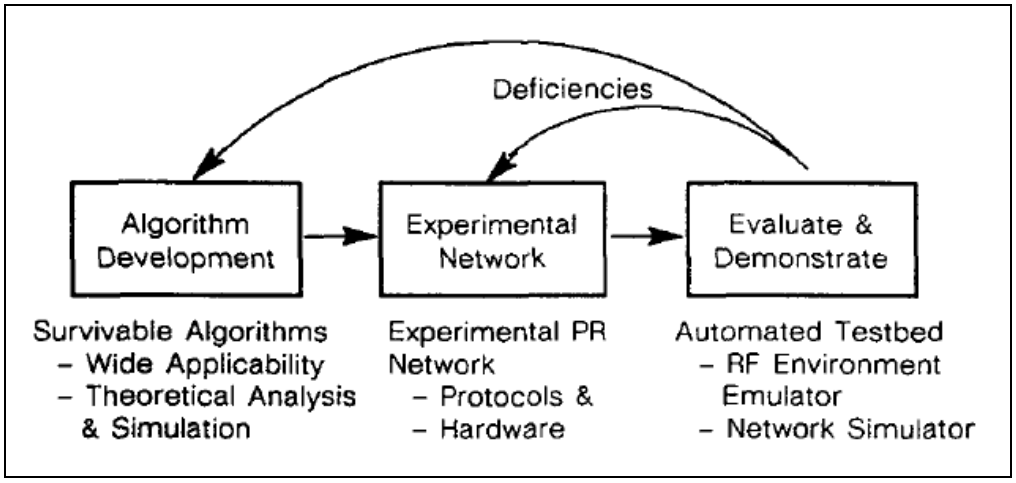

Figure 1. SURAN Program Method of Approach From [4]

Figure 1 also depicts the SURAN method of approach.

3. Third Generation Ad Hoc Networks

Third generation ad hoc networks emerged in the 1990s, and we continue to use them today. Two important technologies arose because of MANETS. These technologies were Bluetooth and Ad-Hoc sensors. Bluetooth came on the scene around 1998 and gave us the ability to support many users in any environment by way of a small network known as a piconet. At any given time, up to ten piconets can exist in the same coverage area. A Bluetooth device can act

as both a client and a server, but a connection must be established before data can be exchanged. This connection is called pairing and must be requested before being established.

In [5], a wireless Ad-Hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data.

Some examples of wireless ad hoc sensor networks are as follows:

- Military sensor networks to detect and gain as much information as possible about enemy movements, explosions, and other phenomena of interest.
- Sensor networks to detect and characterize Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) attacks and material.
- Sensor networks to detect and monitor environmental changes in plains, forests, oceans, etc.
- Wireless traffic sensor networks to monitor vehicle traffic on highways or in congested parts of a city.
- Wireless surveillance sensor networks for providing security in shopping malls, parking garages, and other facilities.
- Wireless parking lot sensor networks to determine which spots are occupied and which are free.

F. NEEDED SOLUTIONS FOR THE TACTICAL ENVIRONMENT

The Special Operations community has a unique mission. It often involves their elite forces being dropped behind enemy lines and gathering critical intelligence in order to support both the nation's defense strategy and often the overall theater campaign's objectives. These missions sometimes put the SOF in situations, or control spaces, where operations may be affected by a loss of connection, obstructed line-of-sight, and/or the need for a restructured data format to maintain optimal communications.

1. Loss of Connection

The first control space exists in the event of an actual loss of connectivity or an impending loss whereby the communications link can be quickly passed to another available network (GPRS, Iridium, Software Radios, etc.) to maintain connectivity. There may be no means of notifying other network users that the platform has changed. Therefore, a software mechanism that automatically adjusts the platforms of other users on the network to ensure constant communication might be needed.

2. Obstructed Line-of-Sight

The second control space would be in the event that obstacles or distance interrupted communications. There would need to be a means for the user at risk to see the range and boundaries of his network. This would allow that user to adjust his/her position in order to maintain communications.

3. Restructuring of Data Format

The third control space concerns the automatic adjustment of the data structure/format. Certain data types are more suitable for specific networks, therefore, as an individual moves from one network to another, there is a need for automatic adjustment of bandwidth and/or security standards.

G. THESIS OUTLINE

Chapter II begins with solutions for MANETs that are more efficient and introduces a new concept of an 8^{th} Layer to the routing protocol stack developed by Dr. Alex Bordetsky and Professor Rick Hayes-Roth, both of the Naval Postgraduate School. Specific routing protocols will be discussed, revealing both strengths and weaknesses for each. Chapter III will specifically focus on Control Based MANETS (CBMANET) as a future network model. Chapter IV will be dedicated to how best to implement a CBMANET into existing Special Operations Command (SOCOM) operations, and a related case study will be discussed in the Chapter V. Finally, Chapter VI will conclude these studies, recommend further actions, and propose future study areas.

THIS PAGE INTENTIONALLY LEFT BLANK

II. STUDIES FOR MORE EFFICIENT MANETS

A. OVERVIEW

The advantages of ad hoc networks have motivated scientists, commercial companies, and government agencies to find ways to solve their latency problem and improve their throughput capacity in order to satisfy continuously increasing user requirements.

In order to achieve this goal, a variety of research has been conducted on different features of wireless networks. There are continuous studies to improve physical layer capabilities such as power consumption, bandwidth, and range, as well as modeling new protocols in network and transport layers that aim to lessen overhead in network traffic. In addition, there is also continuous improvement in the application layer that decreases the required bandwidth by coding data as it is used in programs such as archive managers and media players.

This chapter briefly explains some of the aforementioned studies and concepts. Each has different approaches, but seeks solutions for the same problem: how to achieve faster, dynamic, reliable, and secure communication with ad hoc networks.

B. 8TH LAYER OF OSI MODEL

In [6], Bordetsky and Hayes-Roth suggest a protocol called the 8th layer of the OSI Model. This protocol reduces complexity, provides fast, self-forming and adaptive networks, increases the performance by utilizing a memory mechanism, and gives an optimized solution depending upon the existing constraints. Critical nodes utilize this model, and each of them acts as an automated Network Operation Center (NOC).

According to Bordetsky and Hayes-Roth, these critical nodes—or “hyper-nodes” as they call them—are expected to improve awareness of the network by

providing self-diagnosis, subnetwork view, end-to-end performance, quality of service requirements response, and negotiation of service level agreements [6].

Each hyper-node with the aforementioned capabilities becomes able to execute the procedure depicted in Figure 2 and helps to establish the communication goals of the entire network. These nodes utilize Case Based Reasoning (CBR) to create a kind of memory mechanism that increases the performance of the network.

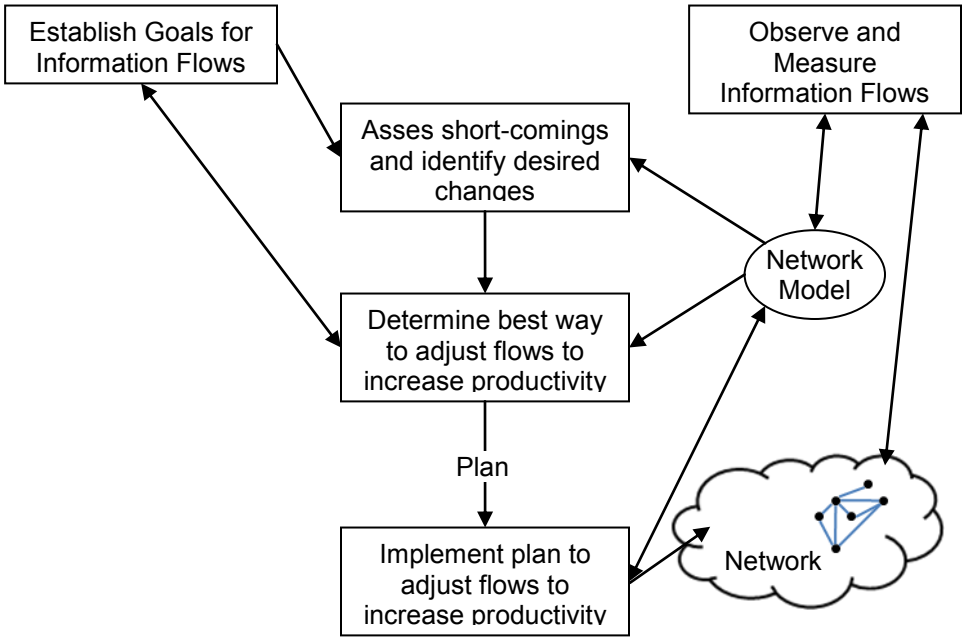

Figure 2. Intelligent Adaptation From [6]

This concept briefly aims to improve the efficiency of ad hoc networks by utilizing artificial intelligence within hyper-nodes in the network, which provides a kind of control mechanism to realize self-synchronization between nodes.

C. INFORMATION THEORY FOR MOBILE AD HOC NETWORKS (ITMANET)

ITMANET is a program running under DARPA. Program manager Lazarus states the mission of the project is “to develop and exploit more powerful information theory concerning mobile wireless networks” [7].

The first objective of the program is to define the capacity limitations of MANETs using a formulation that will include not only known variables like signal to noise ratio and bandwidth, but also variables like energy, latency, computation, mobility, traffic characteristic, topology, overhead, and node heterogeneity [8]. MANET’s capacity limits are not obvious, and their capacity depends intricately on interference, mobility, delay tolerance, and electromagnetic transmission phenomena [9].

The second objective is to benefit new and emerging technologies [8].

In general, ITMANET aims to learn more about the capacity limits of MANETs so that the combination of learned information and new developments can provide solutions to the current problems of MANETs.

D. SOFTWARE DEFINED RADIO (SDR)

Adaptive ad hoc networks require flexible nodes that can be provided by implementing SDRs. Therefore, SDR approach is an important milestone in improving MANET’s efficiency. DoD carries out this objective with the Joint Tactical Radio System (JTRS) Program.

JTRS is a transformational program that will replace the DoD’s aging radio systems with a family of revolutionary Software Defined Radios (SDRs) [10], [11], [12], [13]. SDRs are more like a computer than a radio. This feature brings high elasticity and provides easy interoperability between SDRs. It reduces the impact of the limited bandwidth and spectrum problems found with old radios.

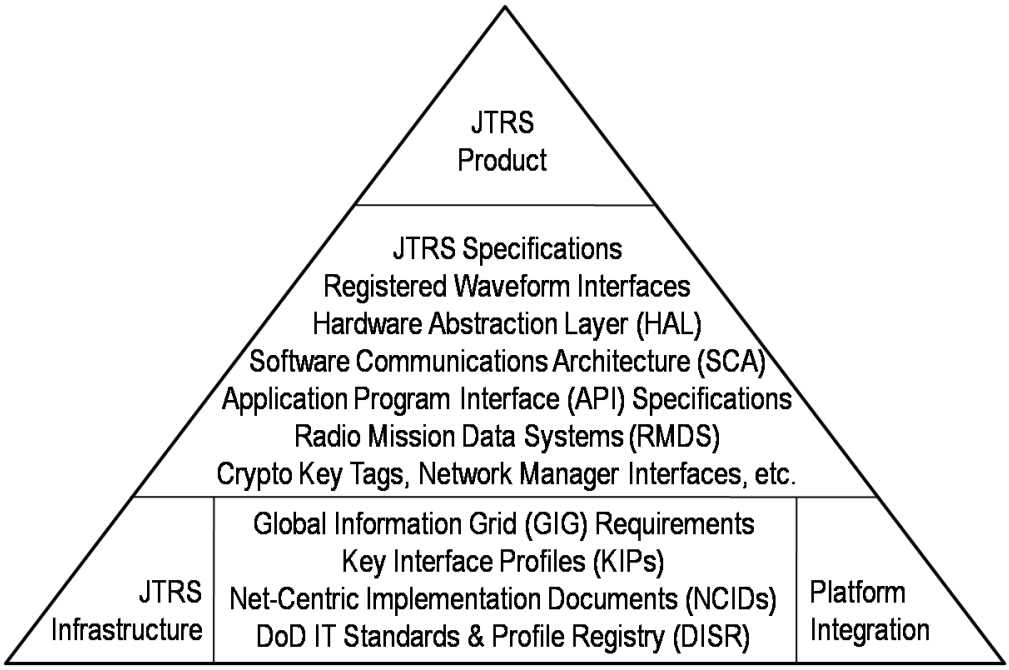

Figure 3. JTRS Common Standards and Specifications From [10]

The goal of this project is to provide interoperability between all radio-systems used in DoD. Figure 3 shows common standards and specifications that create the basic features of products, which provide interoperability.

JTRS also comes with its own network management capability. JTRS Wideband Network Manager (JWNM) and JTRS Enterprise Network Manager (ENM) will provide network configuration and monitoring [10]. This management feature will provide a common picture of any network that uses SDRs and help to increase network efficiency.

E. APPLICATION LAYER

Another way to solve the bandwidth problem is to change the bandwidth requirements of the application we use. Dynamic protocols monitor the bandwidth resource of the network and change the application's features, which results in a reduction of data that needs to be sent. These protocols cannot solve the problem completely, since they have limitations. They can only reduce the

bandwidth requirement to a certain threshold, and, if the threshold is exceeded, the connection gets lost. Below are two examples that use a dynamic bandwidth approach:

1. Dynamic Voice-over IP (DVoIP)

Any military environment is very likely to have different networks with different bandwidth capacities. As VoIP data pass through these networks, it cannot adapt itself to different bandwidth environments, and it ends up with reduced QoS or a loss of connection. DVoIP allows VoIP streams to pass through heterogeneous networks by reducing the bandwidth requirements of a VoIP packet [14].

It provides the adaptation at any given time, by changing the parameters of the audio transcoder and frame aggregator to specific values that require a desired bandwidth level [14].

2. Situational Aware Protocols in Edge Network Technologies (SAPIENT)

SAPIENT is another program running under DARPA to ease the bandwidth problem in tactical networks.

For this project, Lockheed Martin developed a solution known as Synthesizing Adaptive Protocols by Selective Enumeration (SYNAPSE). SYNAPSE functions as a bridge between the red side router and encryptor. It monitors the network bandwidth capacity and provides adaptation by choosing an appropriate protocol from list below [15].

- Flow Mux/Demux
- IP
- Application Detection
- TCP Proxy
- Traffic Management
- Adaptive Sliding Window

- Application Performance Classifier
- Queue
- Network Aware VoIP
- Packet Aggregation / Fragmentation
- Dynamic Information Dispersal Algorithm
- SynVent (application specific optimization for Army)

Figure 4 depicts the implementation of SYNAPSE. As the bandwidth resource decreases, SYNAPSE switches to another protocol that requires less bandwidth. It informs the other SYNAPSE box on the remote site by adding a specific header to each packet.

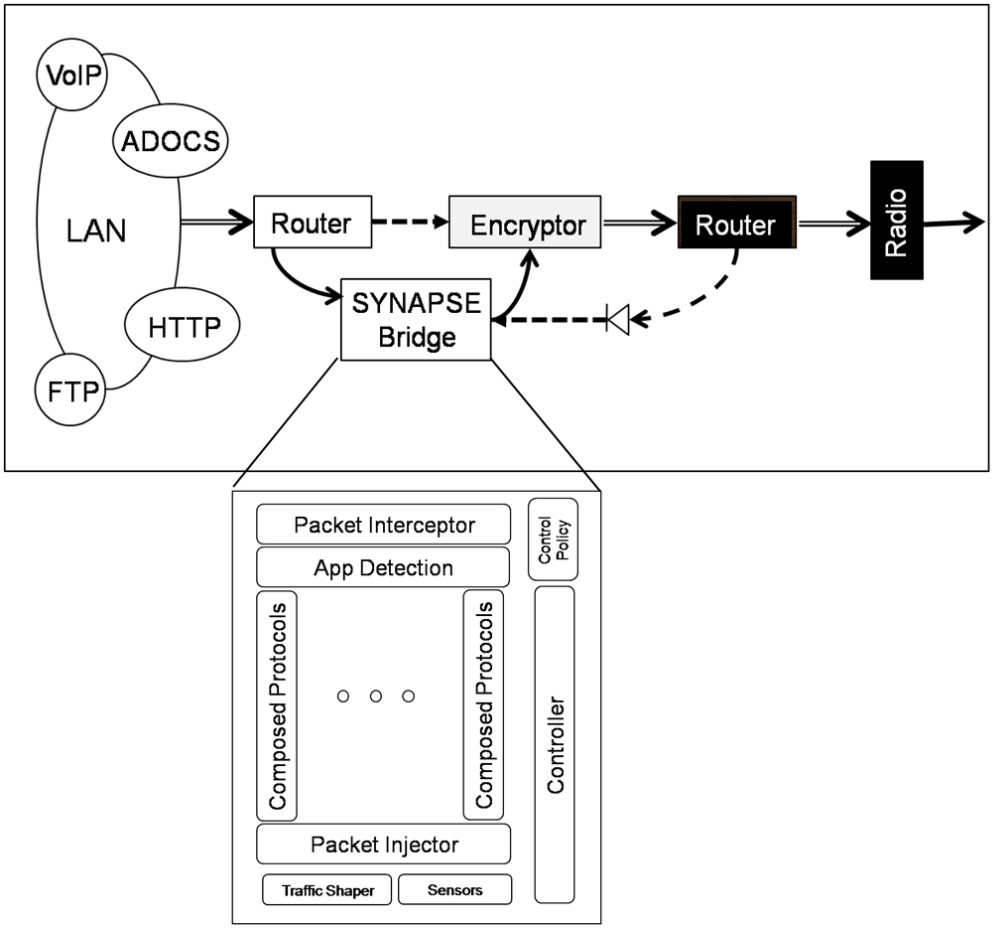

Figure 4. SYNAPSE Implementation From [15]

Another feature of SYNAPSE is that, after sending a file to a remote site, it only sends the changes that have been made to that file. For video streaming, at first it sends a full frame and then only the differential from the previous one. This feature drastically reduces the requirement of bandwidth.

For voice communication, SYNAPSE utilizes the human factor. In fact, voice communication does not necessarily require high quality. To a certain degree, low quality still provides clear voice communication. When bandwidth decreases, SYNAPSE reduces quality of voice communication to let the packets pass through the network easily, and this keeps communication alive.

F. NETWORK LAYER

Two scarce resources for ad hoc mobile nodes are energy and bandwidth. In order to solve these two problems, many studies on routing protocols have been conducted and more are ongoing. The main goal of these studies is to enable data travel through the shortest path from source to target host. Achieving this goal will lead to a reduction of overall energy consumption and traffic on the network.

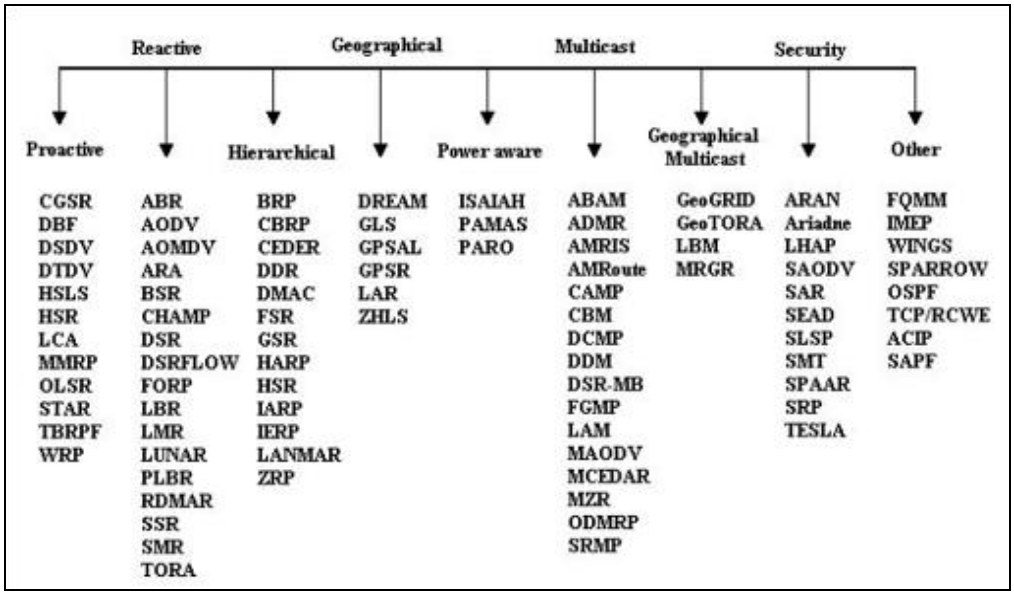

Figure 5. Ad-Hoc Routing Protocols From [18]

There are different approaches to classifying routing protocols. Some sources [16], [17] use table driven and on-demand routing classification; others [18], [19] prefer proactive and reactive classification, and in [20], [21], we can also find hybrid routing protocols as a third approach to this classification.

Figure 5, drawn by Halvardsson and Lindberg [18] in 2004, shows a good classification of ad hoc routing protocols. However, it is very hard to keep that kind of list up-to-date. New protocols that aim to increase the efficiency of mobile ad hoc networks continuously come out. Enhanced Power-Aware Routing, which aims to decrease the energy consumption, is one of them [22]. DPUMA, another new protocol that Figure 5 does not list, is a mesh-based highly efficient multicast routing protocol, which is specifically designed to save bandwidth and energy by reducing the overhead needed to deliver multicast packets [23]. SAFAR, which aims to optimize the usage of bandwidth, is also not on the list [19]. As this paper is written, more research is being done to develop better routing protocols.

Since evaluating every routing protocol is beyond this study, this chapter will discuss three types of routing protocols, as they are used ad hoc mobile networks.

1. Proactive/Table Driven Routing Protocols

In this approach, every node in the networks has one or more routes to transmit or retransmit data. Nodes need to maintain their routing tables constantly; therefore, they continuously exchange routing information. This function creates network congestion and takes a lot of bandwidth [18]. On the other hand, in these types of protocols, nodes send data with no delay.

Proactive protocols are not commonly accepted for ad hoc networks since they increase network traffic [19]. In high tempo tactical operations, some variables about nodes, such as the number of users in the operation area and

their position to change continuously, are expected. In this case, heavy data traffic to keep routing tables up-to-date, will consume our scarce bandwidth resource.

2. Reactive/On-Demand Routing Protocols

In reactive routing protocols, routing information on nodes is not periodically updated. When a node wants to send data to another node, it initiates a route discovery process if it is not a known route [16], [17], [18], [20], [21]. This provides the following advantages over proactive routing protocols [18]:

- Lower bandwidth usage for control traffic.
- More energy-efficient.
- Effective route maintenance.

However, even with these advantages, an on-demand routing discovery process creates unavoidable latency in communication [18], [21].

Reactive protocols have similar nature to ad hoc networks; therefore, they seem to be appropriate protocols for MANETs. However, their latency problem motivates scientists to develop and implement hybrid protocols in ad hoc networks.

3. Hybrid Protocols

Researchers have developed hybrid protocols to use the advantages of both reactive and proactive protocols. Each node acts proactively in its determined zone, and reactively outside the zone [17], [21]. This addresses the issues of both latency and control traffic on the network. In other words, it reduces network traffic by implementing reactive protocols outside the zone, and reduces latency by implementing proactive protocols inside the zone.

G. PHYSICAL/DATA LINK LAYER

There are also many studies being done on the first and second layers of the OSI model. Most of them focus on increasing the bandwidth provided by the

physical layer protocols. Efforts to develop antennas that are more efficient are in progress as well. As discussed below, simultaneous improvements in the first two layers and antennas help to increase the efficiency of MANETs.

1. 802.11n with Multiple Input Multiple Output (MIMO) Technology

The goal of the 802.11n amendment is to increase the throughput and the range gained with 802.11a/g. Task Group n (TGn) initially aimed to provide at least 100 Mbps throughput [24], [25]. As explained in draft amendment, making enhancement in both physical and medium access control layers will help achieve this goal [25]. The key element in this enhancement is MIMO technology.

MIMO technology uses more than one antenna at the same time, which is completely different from diversity that uses only the antennas that gets the best signal [23, [26]. MIMO uses a spatial-division multiplexing technique that allows for multiple data streams on the same channel by using multiple antennas [25], [27]. Unfortunately, MIMO capacity does not increase as we increase the number of antenna. Statistical properties and antenna element correlations of the channel are the elements that affect MIMO capacity [28].

802.11n will be based on 802.11a amendment and use High Throughput OFDM (HT-OFDM) [26]. Expected maximum result is 600 Mbps [26]. The draft mentions three modes of protocol: non-HT mode, HT mixed mode, and Greenfield mode [26]. The first two modes will provide backward compatibility.

Although 801.11n amendment has not been ratified as we write this chapter, many places, especially universities, have implemented 802.11n networks [27]. This is an obvious indication of the urgent need for either more bandwidth or more efficient usage of the spectrum.

2. 802.16 with Self Aligning Feature

802.11n will provide more bandwidth, but only for relatively short distances. 802.16, also known as WIMAX, helps to meet the distance

requirement with high bandwidth. Initial 802.16 standards have a 10-66 GHz frequency range and operate over line-of-sight (LOS) paths. Its expansion, 802.16a, has a 2-11 GHz frequency range and operates over LOS and non-line-of-sight (NLOS) paths [29]. It provides data speed up to 75 Mbps, low latency, efficient use of spectrum space, and 30 miles maximum range with throughput degradation [30].

A very good example of its implementation is the backbone of the Center for Network Innovation and Experimentation (CENETIX) Tactical Network Topology (TNT) test-bed [31]. In the current TNT test-bed, 802.16 links provide up to 54 Mbps bandwidth with maximum distance of 62.58 km [31]. This powerful network acts as an transparent bridge between end users and networks. As an ad hoc network establishes a connection to TNT test-bed at any point, users of the ad hoc network find themselves in a network of networks, that is to say one user can communicate with any other user connected to the TNT.

Figure 6. First SAOFDM From [31]

In order to attach ad hoc networks successfully to TNT type backbones by implementing 802.16 technology, links need to be established quickly. However, in long distance communications, aligning directional antennas is time consuming. In tactical operations, this issue becomes very important. Self Aligning OFDM (SAOFDM) is one solution for that problem. Figure 6 shows first SAOFDM.

SAOFDM uses a control link in order to provide a self-aligning feature [31]. A control link can be a 900 MHz link or an “out of band” link (GPRS, Iridium etc.), which carries position (GPS) and Received Signal Strength Indicator (RSSI) information and changes according to the environmental variables such as distance between nodes, positions of the nodes, obstacles in the terrain, and interference [31]. If there is a problem with the 900 MHz link connection, a low-bandwidth link is an acceptable back up whenever, and wherever, there is a service provider. As a control link feeds information about a remote node, a self-aligning unit rotates antenna to the calculated angle for higher RSSI [31]. Figure 7 shows control link communication devices used with SAOFDM.

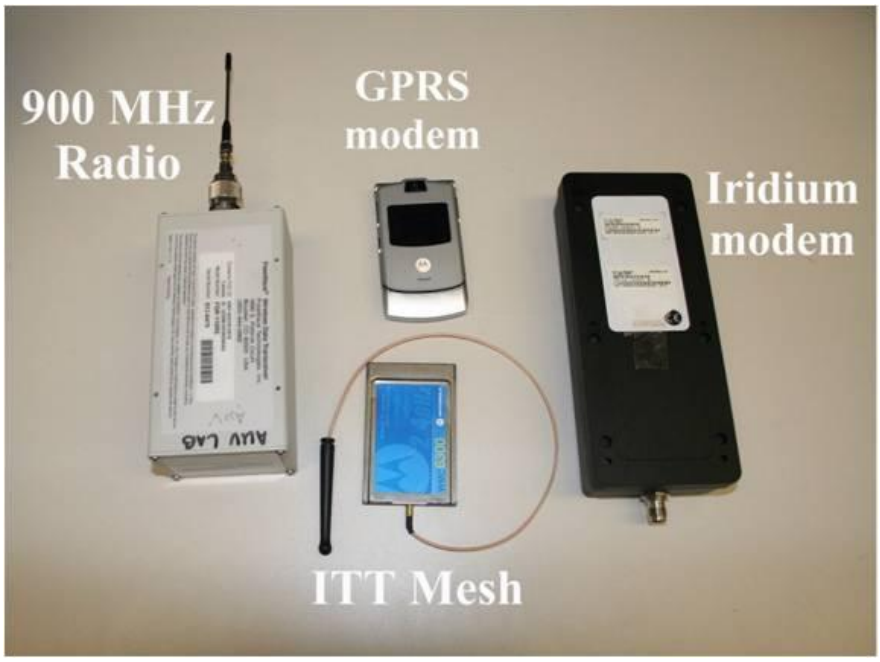

Figure 7. Control Link Communication Devices From [31]

As mentioned in [31], SAOFDM “makes self-forming on demand networking with unmanned vehicles feasible and rapidly deployable.” It increases MANETs’ capabilities by quickly establishing long distance, high bandwidth communications.

3. Ultra Wide Band

Initially, radar based applications used Ultra Wide Band (UWB) technology. However, increasing bandwidth requirement led researchers to think of UWB as another solution.

UWB signals have the following features [32]:

- High performance in multipath channels
- Low transmit power
- Transmitted UWB signal is capable of penetrating through multiple 12" thick concrete walls

In addition, two main characteristics differentiate UWB systems from others. UWB has more than 25% of a center frequency, or more than 1.5 GHz. bandwidth, which is very large compared to other technologies [33]. Another characteristic of UWB is carrier signal. UWB does not use carrier signals to transmit data. It can directly modulate data signals [33].

In [32], possible applications of UWB can be found as follows:

- Secure communications for military operations
- Wireless sensor networks for environmental, medical, military, and commercial applications
- Wireless communications between multimedia devices in home entertainment applications

Figure 8 shows the superiority of UWB over other standards by means of spatial capacity. This was published in 2001; therefore, 802.11n and 802.11g do not appear on this figure. This illustrates how quickly wireless technology improves. Although 802.11n has not been ratified at the time of this paper’s writing, pre-n implementations show that it will have at least as much spatial capacity as UWB.

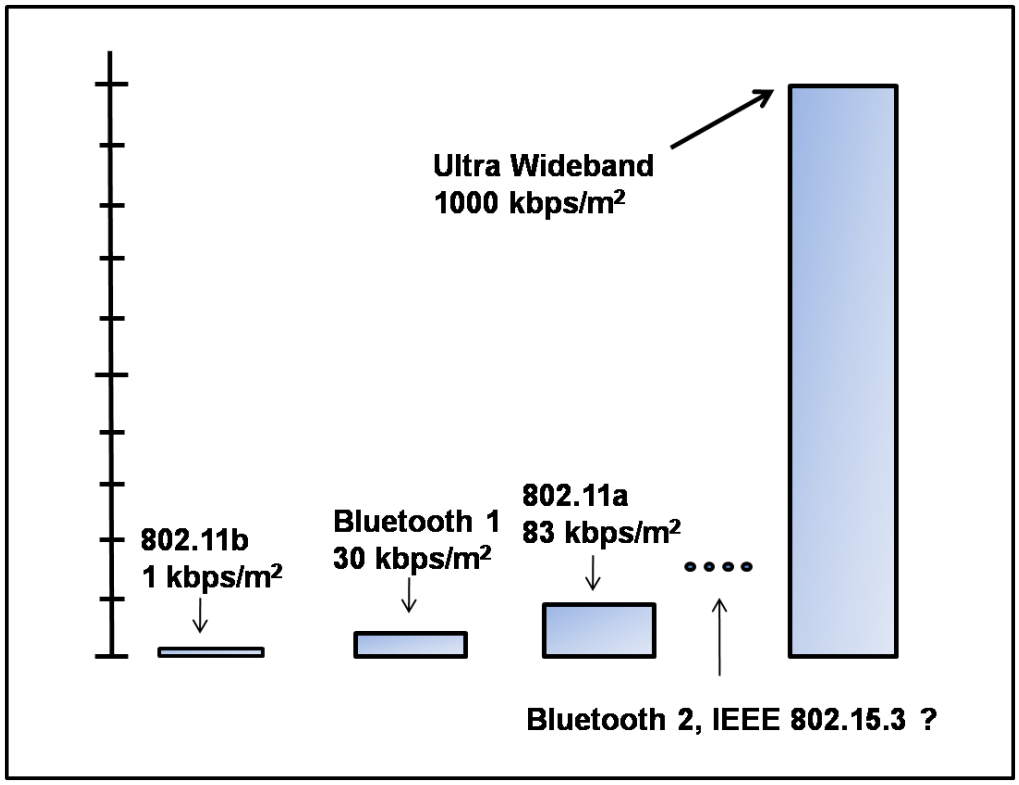

Figure 8. Spatial Capacity Comparison From [33]

UWB provides high bandwidth for current and future communication requirements. However, it is more likely that 802.11n will be more popular, and that will decrease the tendency to seek solutions in UWB.

H. CROSS-LAYER DESIGN

A Cross-layer approach brings the idea of providing nonhierarchical communication between layers. Cross-layer processing, also called interlayer processing, uses at least two OSI layers. By inter-communicating between these layers, it provides vertical optimization [34], [35, [34] classifies cross-layer proposals into three categories:

- TCP and network cross-layer
- TCP and physical cross-layer
- Network and physical cross-layer

Contrary to layered design approach, cross-layer provides more efficient network resource utilization and better QoS provisioning [34]. By using the lower layer channel information, it is possible to increase the throughput and decrease the delay in an ad hoc network [35], [36].

Figure 9 shows a proposed system diagram for a cross-layer framework. This framework increases the efficiency of ad hoc network by incorporating adaptation across all layers of the protocol stack, which gives the flexibility offered by joint optimization of design parameters [37].

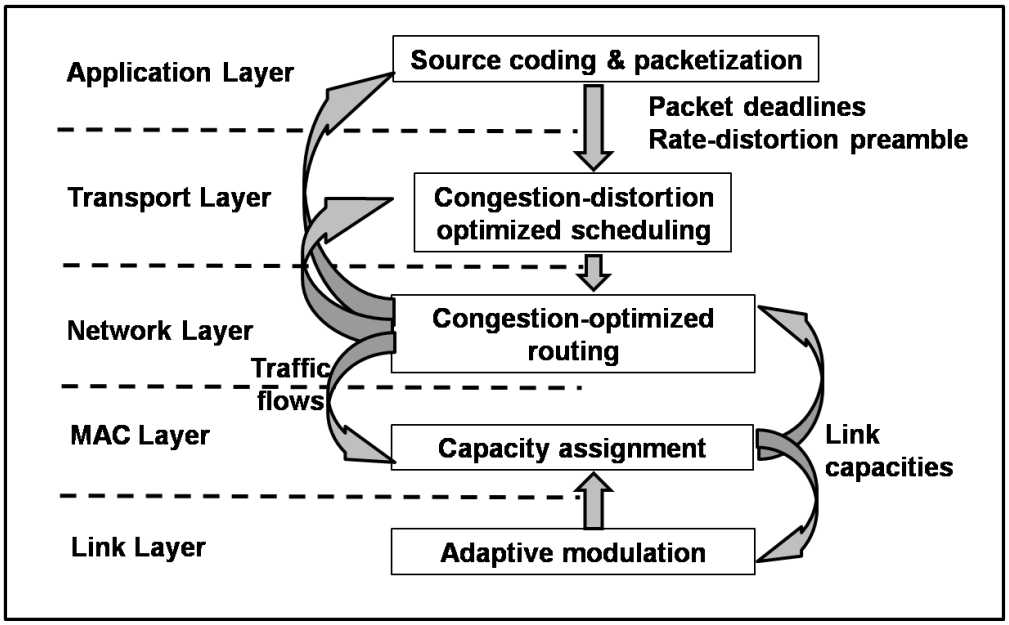

Figure 9. System Diagram for the Cross-Layer Design Framework From [37]

This also allows the exchange of relevant information such as link capacities, traffic flows, packet deadlines, and rate-distortion preamble of the source data across the entire protocol stack [37].

A cross-layer approach is commonly implemented in recent routing protocols in order to realize adaptive networks. Although cross layering improves the efficiency of MANETs, choosing the right architecture is a problem for MANETs used in tactical operations [38]. Figure 10 shows different cross layer applications.

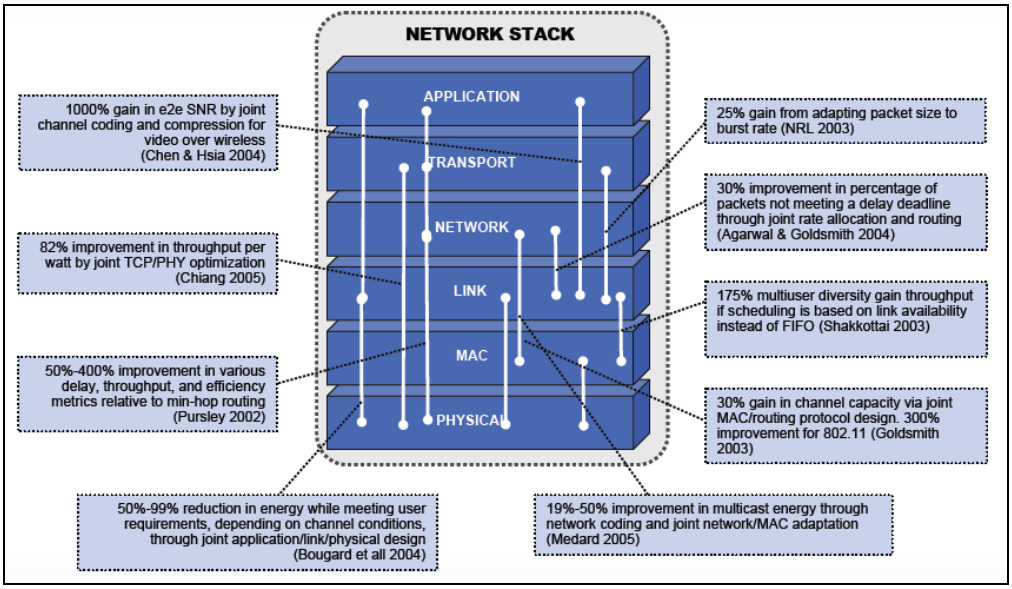

Figure 10. Different Cross-Layer Applications From [38]

I. HOLISTIC APPROACH

So far, most of the studies, projects, and recommended solutions are limited or focused on a specific OSI layer. Improvement in one layer might be restricted by the limitations of another. Although a cross-layer, Approach seems to overcome this problem, choosing the correct cross-layer architecture is an issue for high tempo tactical operations taking place in frequently changing environments.

All this consideration leads us to a new solution for future network requirements; a mechanism, newly designed for MANETs, to control all layers in a stack simultaneously. The CBMANET project is a good example of such a solution. It seeks solutions for efficiency problems with ad hoc networks by creating a brand new protocol stack. The next chapter will discuss more about CBMANET.

III. CBMANET AS A FUTURE NETWORK MODEL

A. OVERVIEW

Wireless ad hoc networks do not require an access point to be established. Nodes in these networks communicate point to point and through other nodes. This feature makes them very attractive for high tempo tactical military operations, since time is usually too scarce to establish a controlled network to support operations.

There is, however, a problem with using a TCP/IP stack in wireless ad hoc networks. TCP/IP stacks were originally designed for wired networks in which bandwidth was not scarce at all. Using them in ad hoc networks reduces the efficiency by utilizing a limited spectrum. In [38], Ramming states spectrum utilization efficiency in wireless networks is less than 11%.

In addition to efficiency problem, characteristics of today's and future military operations put more burdens on MANETs. In military operations, especially in special operations, there are myriad variables that need to be considered. These include force structure (number of nodes in that mission, type of nodes, interoperability of nodes in a joint or coalition operation, distance between nodes, and other technical features), mission profile (goal of the mission, its duration, speed, joint or coalition operation), environmental conditions (terrain, weather, electromagnetic radiation, interference), and enemy. The number of variables changes depending on where, when, and how the operation is conducted; moreover some of the variables might need modification during the military operation. No fighter on the battlefield can deal with all of these variables while conducting his/her mission.

According to the Network Centric Warfare (NCW) concept, in order to establish an infostructure that will realize self-synchronization between nodes, a ubiquitous network is required [39]. For future ubiquitous MANETs, the model

with a unique protocol stack currently stands out as a preferred solution. It will control all of its layers simultaneously and automatically according to different variables and utilize the spectrum more efficiently.

With its innovative and revolutionary approach, CBMANET emerges as a candidate for such a model.

B. CBMANET PROGRAM

CBMANET is a project running under DARPA. It started in 2005 and its projected finish is 2009. It is being developed in two incremental phases. The first phase started in June 2006 and ended in December 2007. The second phase started in March 2008 and ended in July 2009 [40]. By the time this paper is complete, the contractor will be working on final steps of the program.

DARPA awarded CBMANET contract to BAE Systems. BAE Systems is leading a multi-disciplinary research team working to develop a successful CBMANET system based on network coding and the principles of control theory [41]. The California Institute of Technology, Cornell University, Massachusetts Institute of Technology, Pennsylvania State University, University of Illinois, University of Massachusetts, and Stow Research are BAE Systems' subcontractors [41].

1. The Goal of the Program

CBMANET intends to provide U.S. military units an adaptive networking capability by improving performance and reducing serious communication failures.

In [42], the goal of the program is "to research, design and demonstrate a revolutionary Mobile Ad-hoc NETwork (MANET) that improves network effectiveness and performance from a military user's perspective by an order of magnitude." This revolutionary network runs over a novel protocol stack that provides integrated optimization and control of all network layers simultaneously [38].

The goal is to provide the same network effectiveness, while using only 10% of the bandwidth used by the government baseline model [43]. Even though in [43] the term “network efficiency” is not described clearly, one can intuitively considered it as the comparison of the amounts of pure data and total network traffic in a specific time period. Figure 11 depicts target and current network effectiveness versus bandwidth utilization. As compared to the government provided model, which refers to the baseline in 2005, a contractor based model, or CBMANET, increases the performance of the network and saves nine-tenths of the bandwidth. This will allow the users in the network to utilize saved bandwidth to benefit other applications or implement complex applications that are likely to be basic requirements for future military communications.

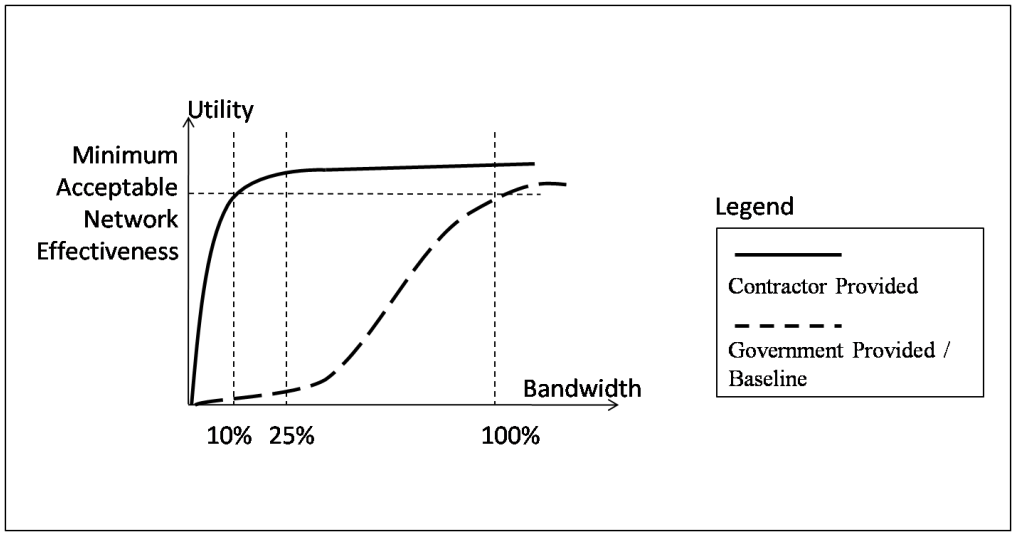

Figure 11. Network Effectiveness vs. BW Utilization From [43]

By increasing utilization of bandwidth, the CBMANET project aims to support DoD applications. These applications can be classified in three groups [44]:

a. Voice

A push-to-talk type of voice communication is required in tactical operations. It is sensitive to packet loss, jitters, and latency.

b. File Transfer

This application provides the ability to share files like maps, presentations, pictures, reports, etc.

c. Situational Awareness

Every user needs to know about the location and the state of the other users. This feature aims to provide a common operational picture.

2. Program Metrics

The goal of the CBMANET program is very difficult to accomplish. In order to track, evaluate, and modify the program's process and prevent any deviation from the goal, researchers should accurately define and continuously assess metrics. As in all other wireless networks, latency, data throughput, and bandwidth usage are important metrics for the CBMANET program. However, for the program, the main metric is network effectiveness [43].

Table 1 shows metric requirements for the CBMANET program. As the table implies, requirements are prioritized and metrics for each phase are determined depending on this prioritization.

Interoperability with legacy networks is not required in the first phase model, but is in the second phase. In addition, no improvement is expected for network initialization time in the first phase. However, in the second phase its threshold decreases by half, from 6 to 3 seconds.

Another difference between the phase requirements is the type required test and demonstration. By the end of phase one, a simulation test and demonstration is accepted. In the second phase, a field test is required as well.

Compared to a baseline model, which uses 100% of the bandwidth, simulation threshold for phase one is 40%, with same efficiency as the baseline. In the second phase this threshold decreases to the goal of the program, i.e., 10%.

Program Metrics	Baseline	Phase 1	Phase 2
Principle Metric: Minimum bandwidth required by the CBMANET as a percentage of what was required by the base line	100%	40% (Simulation Threshold)	10% (Simulation and Field Test Threshold)
Conditioned on: Comparable network effectiveness	Network meets requirements of the offered load and/or the network supports the networks load as effectively as the baseline using a comparative utility-based methodology.		
Number of network nodes	30	30 (Simulation)	30 (Hardware) 30/50/130 (Simulation)
Interoperability with legacy networks demonstrated	Yes	No	Yes
Network is robust to the addition of a new application	Yes	Yes	Yes
Network initialization time	<6 min.	<6 min.	<3 min.
Node entry time	<30 sec.	<30 sec.	<15 sec.
Detect node exit time	<10 sec.	<10 sec.	<10 sec.

Table 1. Program Metrics From [43]

Table 1 also implies that a scalability quality attribute is not a high priority requirement. Since CBMANET is a program for in tactical operations, 30 is a good number of users, and, therefore, it is kept the same in both phases.

Node entry time is another metric that requires improvement. In the second phase, it is reduced from 30 to 15 seconds. Having shorter node entry time allows new users to connect to the network and communicate with existing users quickly. It also increases the performance and the reaction of tactical units, which is a desired feature for today's high tempo operations.

3. Protocol Stack and Algorithm

The CBMANET program aims to have a brand new protocol stack that will manage all of its layers simultaneously in order to increase performance to the required level. Figure 12 shows the comparison of CBMANET and the government provided baseline model.

As the figure depicts, a CBMANET is to be free from any physical layer (PHY). Its algorithm works on a wide range of PHY and Media Access Controls (MAC) [40]. This feature will enable the CBMANET to be used by myriad types of existing wireless platforms and with the ones that will be developed in the future.

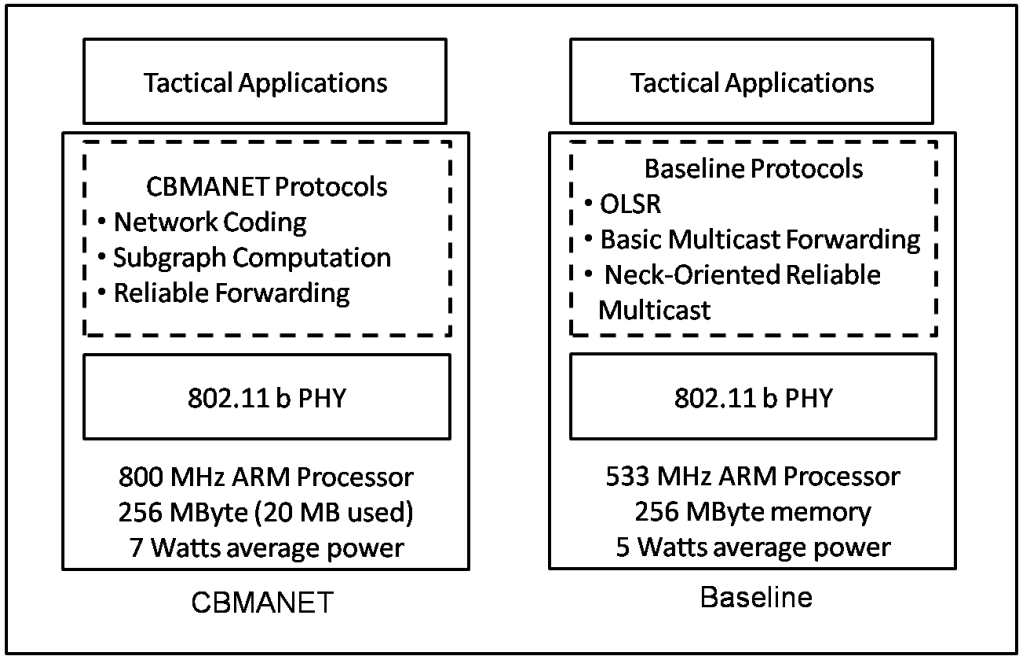

Figure 12. CBMANET-Baseline Comparison From [40]

By the end of the first phase, the CBMANET model appeared to have a brand new protocol stack with ten layers. New layers are listed in Table 2. The authors, for convenience, placed the numbers in the table; they do not show the official order of the CBMANET protocol stack layers.

Layer Number	Description
1	Applications
2	NORM Reliable Transport
3	Flow Admission Control
4	Multicast & Unicast Routing
5	Multicast & Unicast Addressing
6	Reliable Next-Hop Forwarding
7	PFQ Packet Scheduler
8	RC-MAC Channel Address
9	Link Rate and Tx Power
10	2.4 GHz Radio (OPNET)

Table 2. Phase 1 Protocol Stack After [38]

Even though detailed information about the layers was not available at the writing of this paper, the names of the layers imply their function. The new stack covers the functions of the seven layers of the OSI model in the sense that it only focuses on and addresses wireless communication features and problems. Table 2 shows that very last layer, which might be thought of as the physical layer of the OSI model, configured as 2.4 GHz wireless. As previously mentioned, CBMANET is designed to be used with different PHYs. 2.4 GHz wireless should be chosen in order to use the same PHY that the baseline uses.

“Reliable Next-Hop Forwarding” stands out as an interesting layer in the new protocol stack. Even though currently no detailed information is available about how reliability is measured, its name suggests that this layer aims to increase the performance and reduce the latency by choosing the best path, i.e., available and shortest path.

The CBMANET uses network coding as a unified framework. This incorporates and organizes other performance enhancing algorithms, like “rateless coding” in which a node only sends if it has information needed by a downstream node [40].

The CBMANET also utilizes opportunistic routing that requires a node to determine next hop before transmission [40]. Network coding caches opportunistic reception information and uses it to deliver packets to destinations more quickly [40]. Figure 13 depicts opportunistic routing.

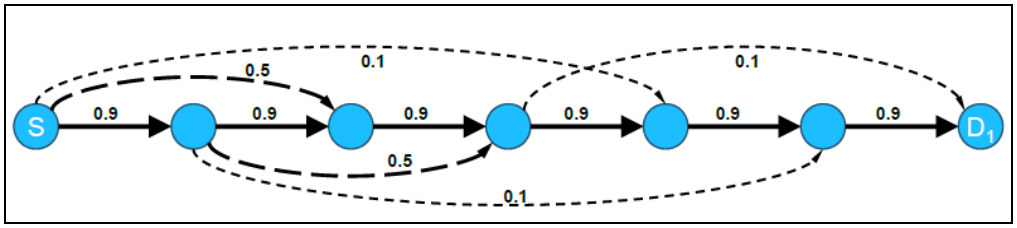

Figure 13. Opportunistic Routing From [40]

Network coding also provides a solution for the “unit link capacity” problem [40]. As depicted in Figure 14, when two sets of data are sent through one unit link, unit link capacity gets violated.

Figure 15 shows how to solve this problem by utilizing network coding. Network coding requires each “per destination” flow to be less than link capacity, whereas routing requires the sum of each “per destination” flow to be less than link capacity [40]. With network coding, CBMANET supports “full rate” multicast to both destinations by XORing packets [40].

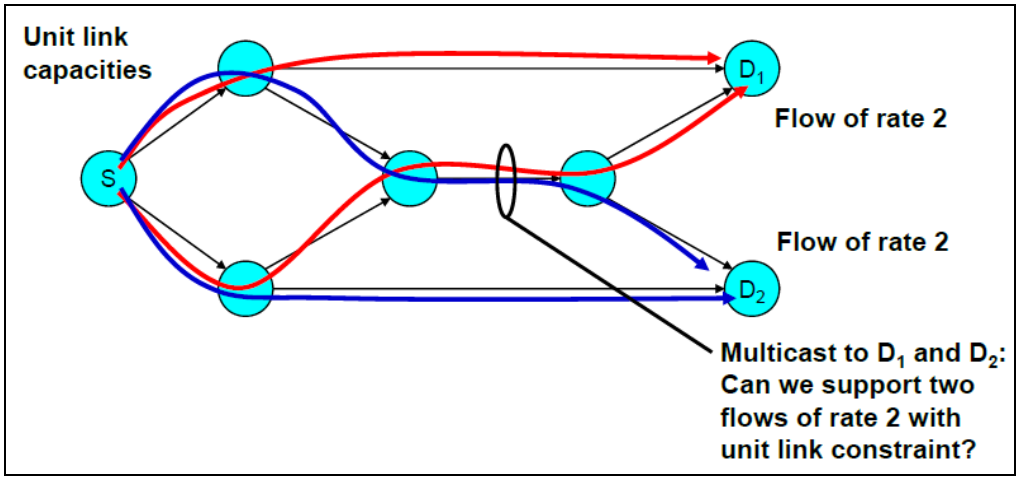

Figure 14. Unit Link Capacity Problem From [40]

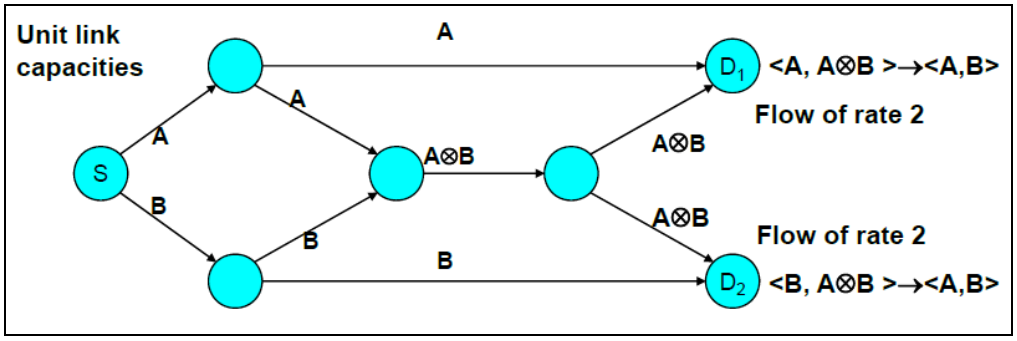

Figure 15. Network Coding for Unit Link Capacity Problem From [40]

In the CBMANET, each node randomly combines the incoming original packets and sends the combinations by adding coefficients in a packet header [40]. Random combination increases the probability of successful coefficient matrix inversion [40]. The receiving node “inverts” the coefficient matrix in the packet header and recovers the original packets [40]. Although it has benefits, this algorithm requires more computational power and puts additional headers on data packets. However, with an exponential increase in the speed of processors, the additional computational power requirement becomes trivial.

4. Phase 1

As program metrics suggest, the goal of the first phase is to reduce required bandwidth while providing the same network utility.

The designed model of first phase overran its determined requirement metrics. Table 3 shows the average principle metric results of first phase simulation test. Results accepted as successful are printed in bold and underlined for convenience.

Description	30 Nodes		Average
	BW	**BWSR**	**300 – 9900**
Baseline Network Stack Performance	11.0	100.0%	**0.90**
Phase 1 Objective	4.4	40.0%	**0.91**
Phase 1 Result – BAE Performance is comparable at 16% bandwidth	2.2	20.0%	**0.92**
	2.0	18.2%	**0.92**
	1.9	17.3%	**0.92**
	1.8	16.4%	**0.92**
	1.7	15.5%	**0.89**
	1.6	14.5%	**0.89**
	1.5	13.6%	**0.87**
	1.4	12.7%	**0.85**
	1.3	11.8%	0.83
	1.2	10.9%	0.80
Phase 2 Objective	1.1	10%	0.76

(BWSR – Bandwidth Savings Ration)

85%-100% - Acceptable average utility
70%-85% - Marginal average utility
< 70% - Unacceptable average utility

Table 3. CBMANET Phase 1 Performance After [38]

Given 11 Mbps bandwidth, the government baseline model provided 90% network utilization. This utilization level is the goal of phases one and two. As noted in Table 1, an average utilization level between 85%-100% is acceptable as a success.

By using 40% of the bandwidth, the CBMANET model provided 91% average utilization, which is 1% more than the baseline model. This result clearly shows that the new model has achieved the principle objective of first phase.

The model is also tested by gradually reducing bandwidth usage to 10%, which is the program's goal. As seen in Table 3, the first phase was successful as far down as 12.7% of the Bandwidth Saving Ration (BWSR) on average. This is very close to the second phase objective.

Table 4 gives simulation results in time intervals. It tells more about the insight of the simulation. As the table shows, for the BWSR values below 16.4%, network utilization deteriorates and the model functions inconsistently. This assumes that no external scenarios are injected in those time units. Also in time interval of 7200-9000 seconds, in other words after two-hours of operation, network utilization decreases significantly and in the next period increases again. If this is not an external effect, which is only taking place during this period, deterioration could be thought of as a fault of the model.

All of the values, other than accepted ones, lie in the range of marginal average utility. Another success of the phase one model is that it has no value less than 70%. It shows that after some optimization and improvement, the program will very likely achieve its goal. On the other hand, the remaining 5% difference to required to achieve the goal might be a very difficult threshold to overcome.

	Average Utility per Scenario Time (periods in seconds)					
BWSR	**300- 1800**	**1800-3600**	**3600-5400**	**5400-7200**	**7200-9000**	**9000-9900**
100.0%	**0.96**	**0.92**	**0.86**	**0.91**	0.83	**0.94**
40.0%	**0.93**	**0.93**	**0.89**	**0.92**	**0.86**	**0.91**
20.0%	**0.90**	**0.94**	**0.94**	**0.95**	**0.86**	**0.94**
18.2%	**0.89**	**0.96**	**0.95**	**0.96**	**0.85**	**0.95**
17.3%	**0.89**	**0.95**	**0.95**	**0.95**	**0.86**	**0.89**
16.4%	**0.86**	**0.94**	**0.95**	**0.95**	**0.85**	**0.96**
15.5%	**0.85**	**0.87**	**0.95**	**0.94**	0.79	**0.95**
14.5%	**0.89**	**0.87**	**0.94**	**0.89**	0.82	**0.95**
13.6%	**0.86**	**0.85**	**0.95**	0.83	0.80	**0.94**
12.7%	**0.86**	0.82	**0.94**	0.83	0.79	**0.89**
11.8%	0.82	0.82	**0.95**	0.77	0.78	**0.89**
10.9%	0.77	0.79	**0.92**	0.73	0.73	**0.93**
10%	0.73	0.70	**0.85**	0.71	0.72	**0.87**

(BWSR – Bandwidth Savings Ration) **85%-100%** - Acceptable average utility
70%-85% - Marginal average utility
< 70% - Unacceptable average utility

Table 4. Detailed CBMANET Phase 1 Performance After [38]

5. Phase 2

Whereas first phase focused on the reduction of required bandwidth, the second phase focuses on increasing a carried load while providing comparable performance, [40].

At the end of the second phase, in June 2009, researchers conducted a field test, as required by program metrics. The test was based on a realistic

hostage rescue operation. The results of the test were declared in the CBMANET VIP Demonstration in Hayes Field near Columbia, MD, on July 31, 2009. Figure 16 shows equipment used by dismount nodes in that demonstration.

Figure 16. CBMANET Phase 2 Demonstration Dismount Unit Equipment

The Field test was based on two scenarios, a ground scenario and an air scenario. The only difference between scenarios was that in an air scenario two Cessna aircraft—assumed as UAV—flew over field during operation. Details about VIP Hostage Rescue scenario are below [40], [45]:

- Each scenario has 3-hour duration.
- Company Alpha with three squads (Alpha, Bravo, and Charlie), supported by battalion aerial assets, is ordered to rescue VIP hostage.
- 35 nodes are used (2 aircraft, 2 trucks, 31 dismounts). (Even though program metric requirement is 30 nodes, in the field test 35 nodes are used)
- During operation, maximum distance between farthest nodes is 1000m.

- Situation awareness traffic is multicast by each node to all other nodes.
- Chat traffic is multicast by each node to all other nodes.
- Files multicast between 7 nodes (one in each cluster, 2 trucks, command post, sensor node), file sizes are ~200KB.
- Three 100 Kbps MPEG video streams from a node in each cluster to other nodes in its cluster are used as video load.

Figure 17 depicts The operation field and starting locations of units. The Operation was executed in the following steps [40]:

- Parking Lot: Nodes gathers in landing zone.
- Deployment: Squads deploy to surround targets.
- Alpha/Bravo: Squads walk around Alpha and Bravo targets.
- Bravo/Charlie: Squads walk around Bravo and Charlie targets.

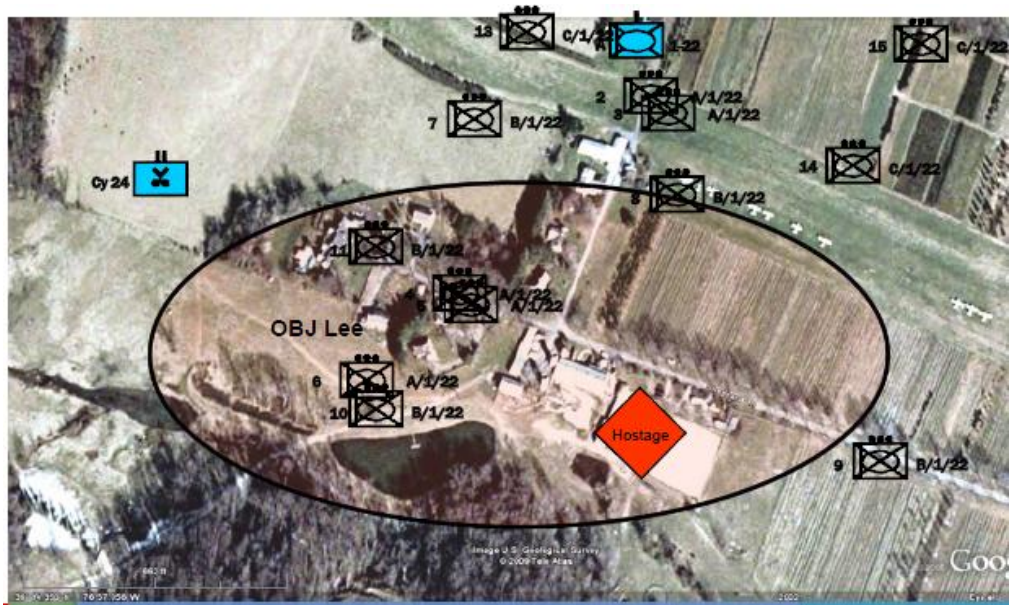

Figure 17. Operation Field and Unit Locations From [45]

The following paragraphs discuss the results of the field tests.

For the destination node, video stream is usable when it gets 90% of the bytes in 10 seconds, and the video utility metric used in the diagrams shows the number of nodes that receive usable video [40].

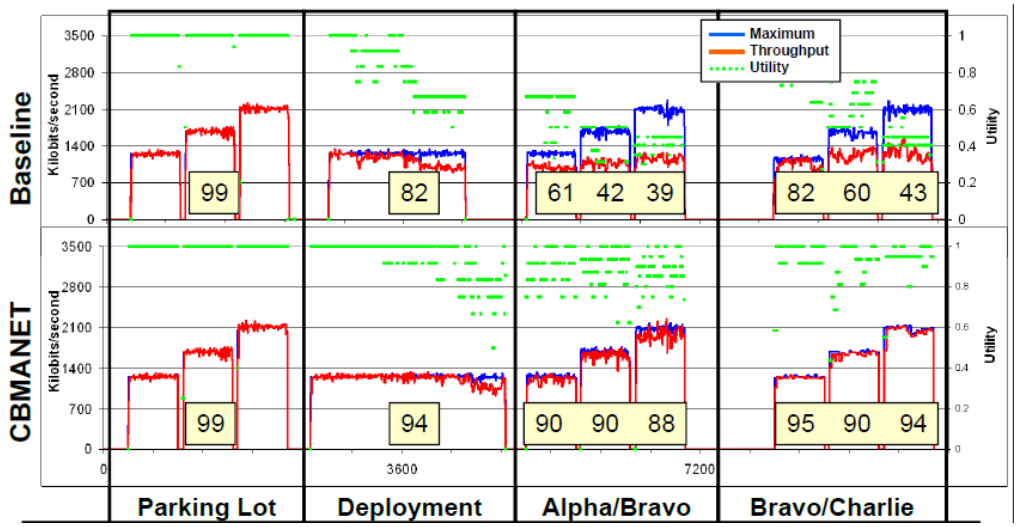

Figure 18. Ground Scenario Video Utility Diagram From [40]

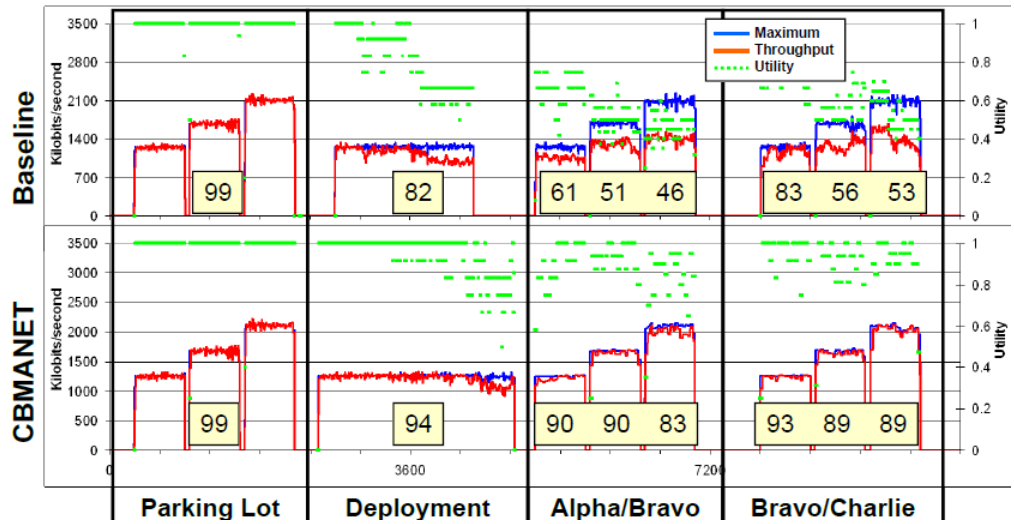

Figure 19. Air Scenario Video Utility Diagram From [40]

Figure 18 shows the ground scenario video utility diagram. In Parking Lot phase, both models have 99% utility. In Deployment Phase, the CBMANET provides slightly more utility with 94%. In the tactical phases, however, the CBMANET shows apparent superiority against the baseline model. In these phases the CBMANET utility only deteriorates slightly, on the other hand, the

baseline utility decreases as low as 39% and becomes effectively unusable. A very similar situation takes place in the air scenario. Figure 19 illustrates the video utility diagram of air scenarios.

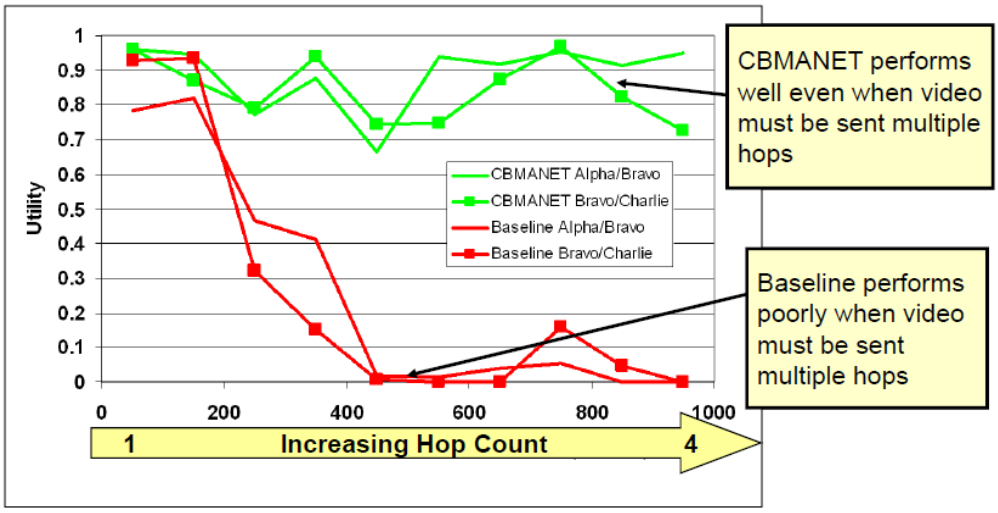

Figure 20. Ground Scenario Utility-Distance Graph From [40]

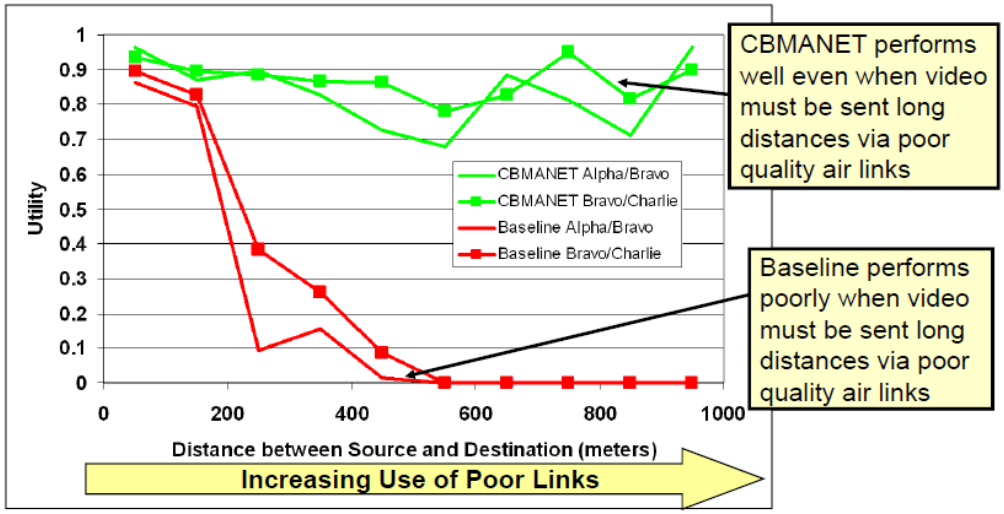

Figure 21. Air Scenario Utility-Distance Graph From [40]

Distance is also an important variable in network performance. As the distance and hop count increase, one expects the performance of the network to

decrease. Figures 20 and Figure 21 show that the CBMANET utility does not deteriorate significantly with a 1000 m distance in both ground and air scenarios. The baseline model utility, however, shows a very extensive decrease at about a 200m distance and becomes zero between 400m and 500m.

File transfer, which is another way for units on the battlefield to share information, is also tested in the VIP Hostage scenario. Table 5 shows the file transfer test results for both models. In each phase of the operation, the CBMANET has 100% success in file transfer, which shows great superiority over the baseline model, especially in the tactical phases.

	Ground		**Air**	
Phase	**CBMANET**	**Baseline**	**CBMANET**	**Baseline**
Parking Lot	100%	100%	100%	100%
Deployment	100%	47%	100%	47%
Alpha/Bravo	100%	26%	100%	16%
Bravo/Charlie	100%	21%	100%	20%

Table 5. File Transfer Results From [40]

As a result, the CBMANET outperforms the baseline model in both ground and air scenarios. It improves performance by seven times over the baseline, and it generates 2–3 times less traffic while providing better performance [40]. Although these metrics are less than the starting goal, this does not overshadow success of the CBMANET.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NEED FOR CBMANET IN SPECIAL OPERATIONS

A. INTRODUCTION TO SPECIAL OPERATIONS

> Today we see a bewildering diversity of separatist wars, ethnic and religious violence, coups d'état, border disputes, civil upheavals, and terrorist attacks, pushing waves of poverty-stricken, war-ridden immigrants (and hordes of drug traffickers as well) across national boundaries. In the increasingly wired global economy, many of these seemingly small conflicts trigger strong secondary effects in surrounding (and even distant) countries. Thus a "many small wars" scenario is compelling military planners in many armies to look afresh at what they call "special operations" or "special forces"—the niche warriors of tomorrow. [46]

In 1987, Congress recognized the uniqueness of special operations and established the SOCOM. Now one of ten Unified Combatant Commands, it is composed of five subordinate commands: USASOC, NAVSPECWARCOM, JSOC, AFSOC, and MARSOC.

Special Operations (SO) is more than the daring, cinematic images we see on our televisions or movie theater screens. Sure, some of it is just as, if not more, thrilling than what we all have come to believe about Special Operations, but it is so much more. Its missions are comprised of a whole host of operations that are conducted in some of the most hostile and politically sensitive environments imaginable.

Special Operations are used to achieve military, diplomatic, informational, and/or economic objectives, and they often require covert, clandestine, or low-visibility capabilities [47]. The saying, no man is an island, definitely holds true for Special Operations forces. It is common for SO forces to work in concert with both conventional forces and other government agencies.

There are some in the world who mistakenly believe SO should be used in every situation. On the contrary, SO forces are to be used as a compliment to and not a replacement for conventional forces. SO differ from conventional

operations in their degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets [47]. In short, SO tactics are called upon to enhance or ensure the overall success of the total theater campaign. Figure 22 graphically depicts the SOF family HQs in the U.S.

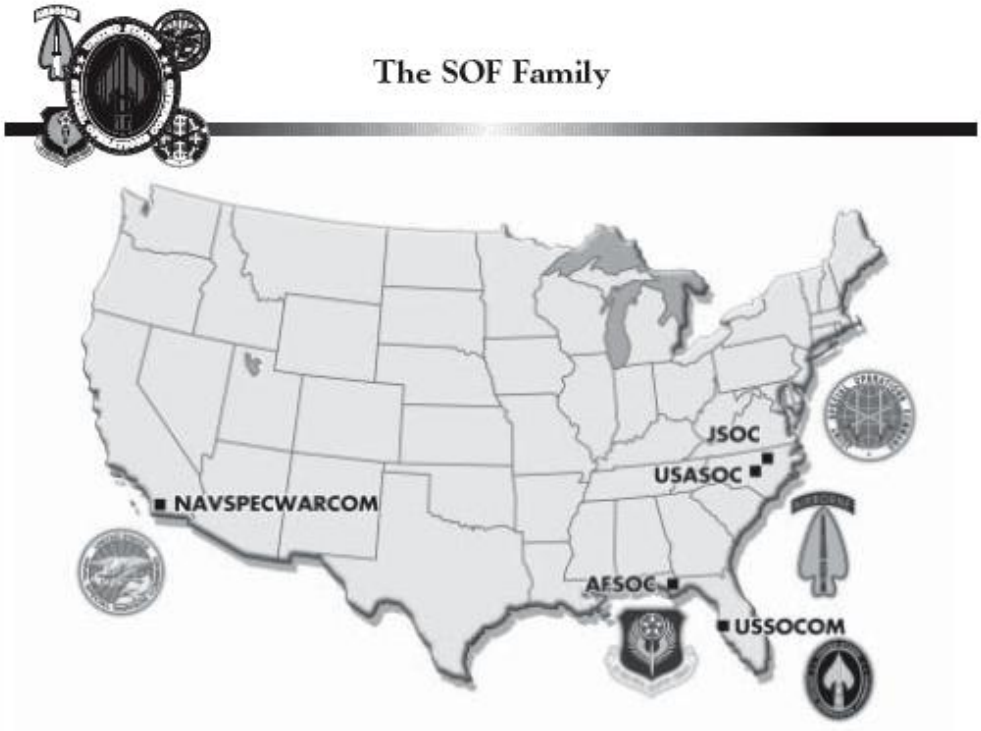

Figure 22. SOF Family HQs From [48]

B. CHARACTERISTICS OF SOCOM OPERATIONS

Special Operations can be and have been employed for a myriad of critical missions. These range from influencing the will of foreign leaders and/or populations to creating conditions that are more in line with US strategic aims and objectives. With that said, there are certain characterizations that distinguish Special Operations from those of conventional forces. Special Operations are defined by nine core tasks [48]:

- Counterterrorism (CT)–CT is the number one mission of SOF and reduces the probability of a successful terrorist attack against U.S. interests.
- Counter proliferation of Weapons of Mass Destruction (CP/WMD)–This refers to actions taken to prevent, limit, and minimize the development, possession, and employment of weapons of mass destruction, new advanced weapons, and advanced-weapon-capable technologies.
- Special Reconnaissance (SR)–Reconnaissance and surveillance actions conducted to collect or verify information of strategic or operational significance using military capabilities not normally found in conventional forces.
- Direct Action (DA)–The conduct of short duration strikes and other small-scale offensive actions to seize, destroy, capture, exploit, recover, or damage designated targets.
- Unconventional Warfare (UW) – Long duration operations involving indigenous or surrogate forces implementing guerilla warfare, covert, clandestine operations, sabotage, and intelligence activities.
- Information Operations (IO) – Actions taken to influence, affect or defend information, information systems, and decision making.
- Psychological Operations (PSYOP) – Conveying truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately their behavior.
- Foreign Internal Defense (FID) – Participation by civilian or military agencies of a government in any action programs of another government to free their society from subversion, lawlessness, and insurgency.
- Civil Affairs Operations (CA)–Establishing and conducting military government or civilian administration until civilian authority or government can be restored or transitioned to other appropriate authorities.

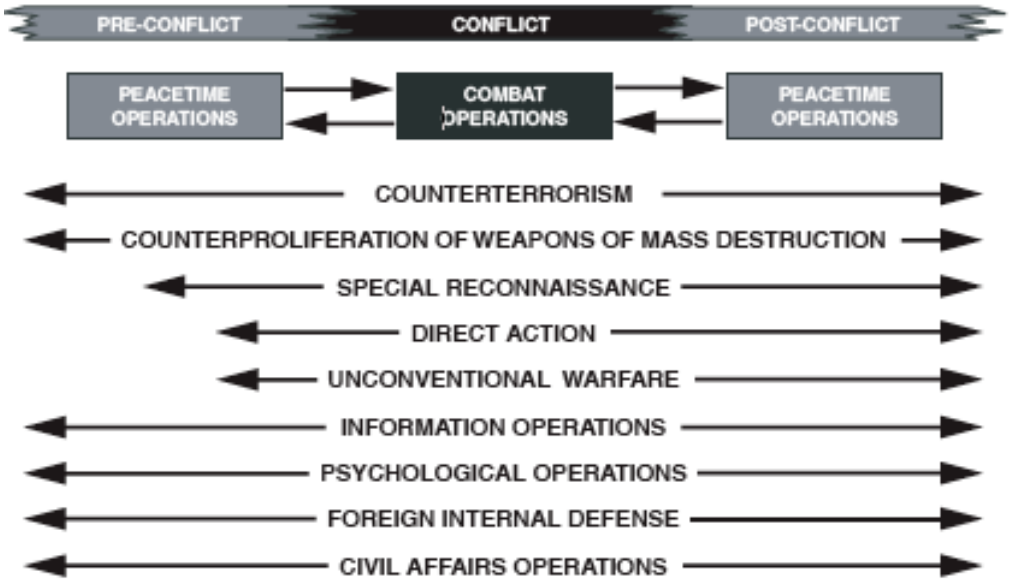

Figure 23. SOF Core Tasks Across the Spectrum of Conflict From [48]

It is plain to see that the activities of special operations are broad across the spectrum and therefore require a special type of soldier, a vast quantity of intelligence, and an enormous amount of planning and synchronization. Even with all of the above stated elements SO still requires a high level of surprise, security, audacity, and deception.

It is standard practice for SOF to thoroughly immerse themselves within the culture and language of their designated area of operation. They must be superbly in tune with the way the native people conduct their day-to-day lives; as they must blend in without causing too much of a disturbance in the community.

In light of their robust mission and the world's changing focus from conventional to unconventional warfare, SOF have to remain on the cutting edge of technology. They should do so, not for the sake of having the latest and greatest toys, but to be better equipped to successfully fulfill the mission of the nation's defensive strategy.

C. SOF COMMUNICATIONS WITHIN A NEW DEFENSIVE STRATEGY

> SOF provides remarkable capabilities for our government – not just as commandos and force multipliers for the Department of Defense, but also as warrior-diplomats increasingly in demand to help carry out foreign policy assignments around the world. [49]
>
> H. Allen Holmes, Assistant Secretary of Defense
> Special Operations and Low-Intensity Conflict

The current unstable world environment has created a greater need for highly trained and superbly equipped Special Operations Forces [49]. Successful SO depends upon three factors: clear national and theater strategic objectives, **effective C4I** and support at the operational level, and competent tactical planning and execution [46].

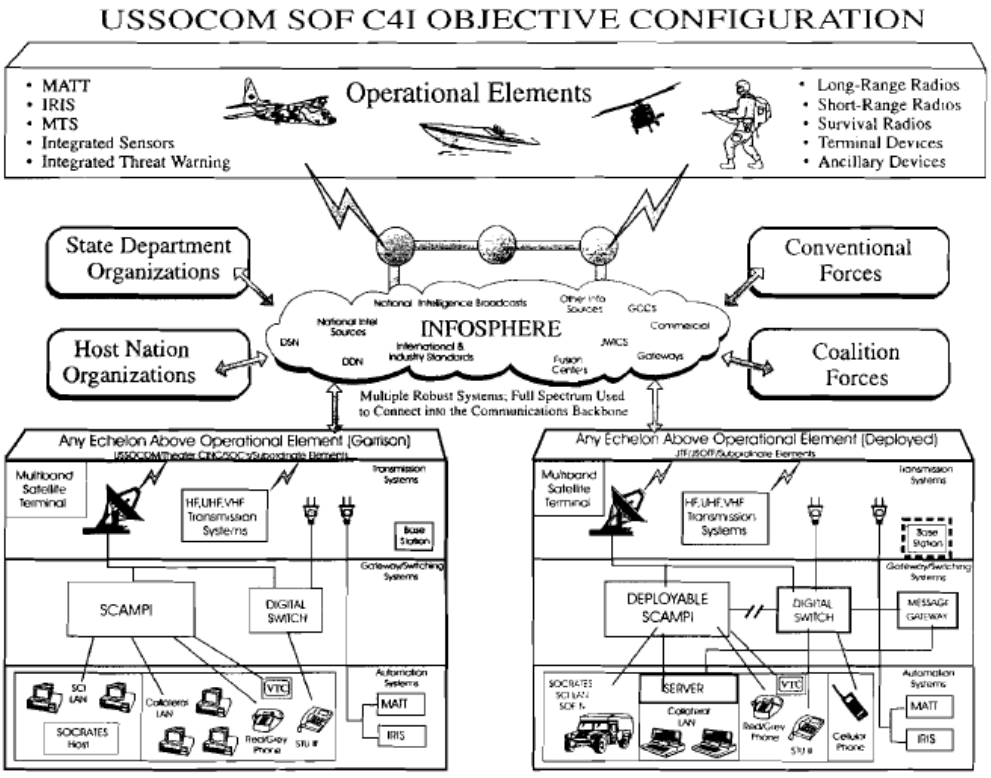

Figure 24. USSOCOM SOF C4I Objective Configuration From [49]

In [49], it is mentioned that maintaining ready, well trained, and technologically advanced SOF is vital to a balanced U.S. defense posture. Figure 24 depicts the overall objective configuration that USSOCOM hopes to realize in the 21st century that will give them the capability to achieve this end.

A configuration of this nature is believed to be capable of providing a worldwide network of interlocking HF base stations. These base stations will, in turn, provide operators access to the infosphere from anywhere in the world. This network will be maintained and controlled by a team of network controllers who will keep the system operationally responsive. Figure 25 depicts a notional worldwide network.

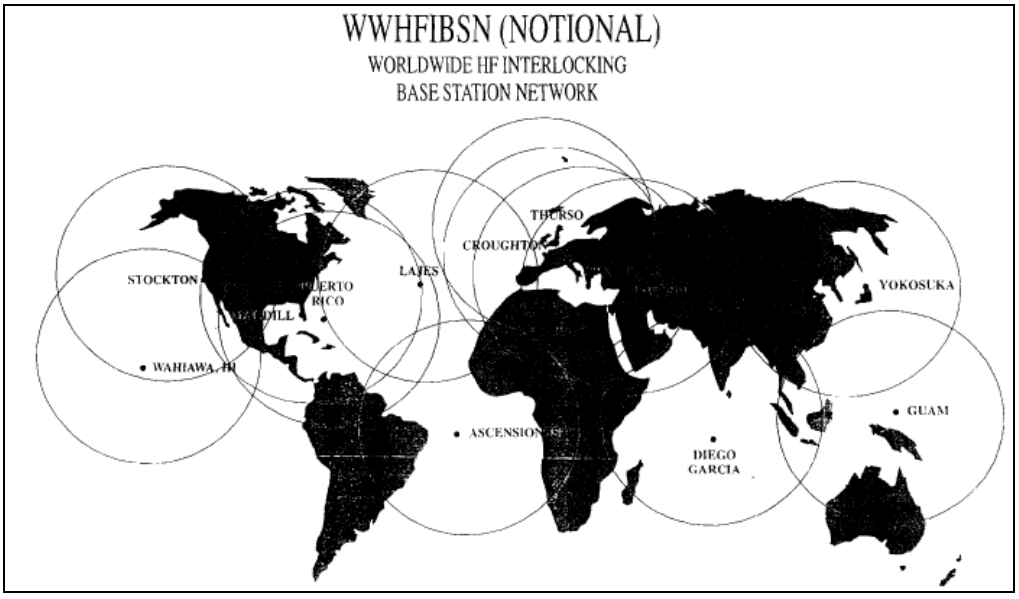

Figure 25. Worldwide HF Interlocking Base Station Network From [49]

The concept stated is where CBMANETs and USSOCOM's objective configuration compliment each other. The CBMANET's self-configuring capabilities and individual node's ability to act as its own router should not only provide stronger links and better use of bandwidth, but also increase the global reach and response time of our forces. With this increased global-reach capability comes a greater ability to defend our nation and secure its interests at home and abroad.

D. SOLVING BANDWIDTH ISSUES FOR SOF

Special Operation Forces have always been on the tip of the spear when it comes to battlefield technologies. They have acquired the best of the best, not because it's nice to have, but because their mission demands it. Special Operation Forces have been and will continue to be required to transmit enormous amounts of data–everything from voice, image, and even large video files. However, SOF cannot continue to be the world's number one fighting force with yesterday's resources and equipment. SOF have to find a better way of transmitting data more efficiently and effectively. It is well documented that transmitting this type of data consumes a huge amount of bandwidth, which in turn can slow the network to a snail's pace.

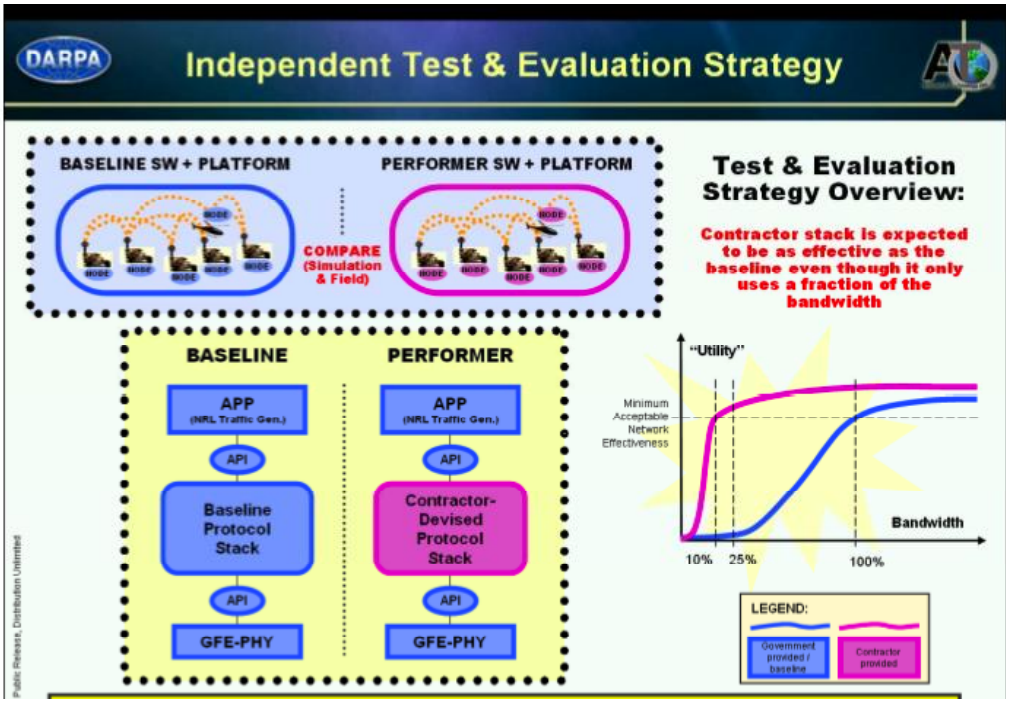

Figure 26. DARPA Modeling & Simulation Test & Evaluation Overview From [43]

DARPA has conducted research in the area of bandwidth optimization and is trying to achieve results that either meet or exceed the current baseline for performance using a CBMANET as depicted in Figure 26. The thought behind the graphic is that if the CBMANET technologies currently being developed allow

for such performance, then the potential effect technologies could have on the SOF community should be very evident.

The characteristics of SOF line up almost perfectly with those of CBMANETs. Therefore, implementing CBMANET into SOF current operations should be quite simple. In fact, the SOF community already has software radios that are compatible with the CBMANET technologies being developed. All that is needed is to mature and further prove the concepts of CBMANET. In Chapter V, a case study will be used to provide a better understanding of CBMANETs and some of the principles discussed thus far.

V. CASE STUDY

A. OVERVIEW

Today, military units are more concerned and involved in Global War on Terror (GWOT) and Operations Other Than War (OOTW) than traditional warfare. Today there are myriad types of operations, in which features are continuously changing. This change is the result of newly improved tactics and enhancement in implemented technologies. Recent operations are agile, relatively short in time, remote (far from TOC/NOC), and usually conducted by small units. Their features are very different from features of traditional warfare. Therefore, permanent communication emerges as a challenging and highly required issue for today's operations.

In this chapter, a Counter Improvised Explosive Devices (C-IED) operation is taken as an example, and CBMANET implementation of such an operation is analyzed.

B. TASK FORCE ODIN

Task Force ODIN (Observe, Detect, Identify, and Neutralize) was a battalion size unit when it was activated in 2007. Its goal was to increase success against insurgent activities and decrease casualties with a proactive approach by providing more intelligence, surveillance, and reconnaissance to U.S. Army commanders [50].

Task Force ODIN consists of two main assets. The first one is the C-12R aircraft, which is designed as either Aerial Reconnaissance Multi-Sensor (ARMS) or Medium Altitude Reconnaissance and Surveillance System (MARSS-II) RSTA platforms specific to the C-IED missions [51]. These platforms are also equipped with some additional unique systems such as, "Constant Hawk," which provides the capability of forensic backtracking, and "Highlighter," which detects changes in a specified path of terrain [51].

Figure 27. A Task Force ODIN ARMS Aircraft From [51]

The second asset of the ODIN Task Force is an “extended range multi-purpose hybrid unmanned aerial vehicle” [51]. Like C-12R, these UAVs are also equipped with special mission specific tools, such as Electro-Optical/Infrared or Synthetic Aperture Radar payloads, Laser Range-Finder Designator, and Laser Target Marker [51].

Figure 28. A Task Force ODIN Unmanned Aerial Platform From [51]

Task Force ODIN also has an Aerial Reconnaissance Support Team (ARST), which provides real time and after action analysis of imagery provided

by C12-Rs or UAVs. The information gathered from that analysis helps Quick Response Force (QRF) to disarm IEDs or capture insurgents while they are planting EIDs.

C. NETWORK REQUIREMENTS

Although there may be myriad numbers of networks and communications established during different operations conducted by Task Force ODIN, this case study focuses on communication between QRF, TOC/ARST, UAV, and ARMS aircraft during C-IED missions.

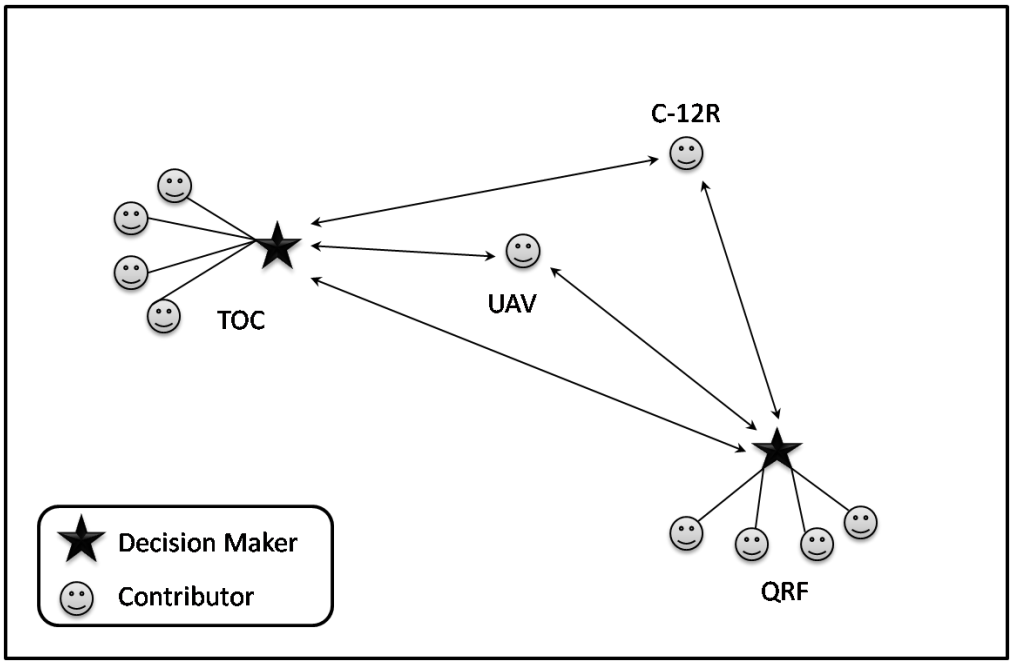

Figure 29. ODIN Decision Support Topology

Figure 29 shows the decision support topology for an ODIN C-IED operation. Both TOC and QRF act as a team. ARST, which may consists of military and civilian experts, might be considered as a committee. However, in this paper it is considered as a part of TOC.

In a typical ODIN C-IED operation, imaginary data captured by aerial assets are transferred to TOC/ARST for analysis. The results of analysis are sent

to QRF to help them quickly make good decisions, act proactively, and be successful. In addition, QRF might need to send some data to be analyzed. The "data" and "results" mentioned here might be text, voice, proprietary file, image, or video streaming. In providing situational awareness, visual information becomes vital for the soldiers in the field. Hence, a network that provides high bandwidth is a requirement for such operations. However, it is very likely that QRF often conducts its mission too far from TOC to have a line of sight communication. Aerial relays need to be established in such situations.

The goal of the aerial assets of the ODIN Task Force is to collect imagery of the concerned area; however, as it can be implied from Figure 29, aerial assets may also function as a relay between two decision makers. The biggest challenge for a permanent network is having aerial relays active and in range during operations. Weather, terrain, flight patterns of the aerial relay, technical features of the network devices, and other known and unknown factors affect the continuity of communication through aerial relays. Any termination during the downloading/uploading of an image causes delay and jeopardizes the success of the operation.

Dismounted QRF personnel need a network that can quickly establish, adapt to changing environments, and provide desired communication between its members and data transfer from TOC. If required, additional force might be deployed to support QRF. In this case, communication between two units needs to be established immediately. In such high tempo operations, soldiers on the field need permanent communication as well. An automated control mechanism to provide continuous and adaptive communication by selecting available channels and devices is vital for fighters while they are conducting their operations.

The critical network issues mentioned above are addressed in CENETIX TNT experiments. A network, similar to the one used by the ODIN Task Force, is established for two purposes. The first is to test the maximum range that can be

achieved and the second is to monitor the network behavior during the experiment. Figure 30 depicts the TNT ODIN Network.

In Figure 30, a proprietary OFDM mesh network establishes the communication among TOC, aerial assets, and QRF. Dismounted personnel use hand held mesh radios to communicate with each other and connect to OFDM mesh network.

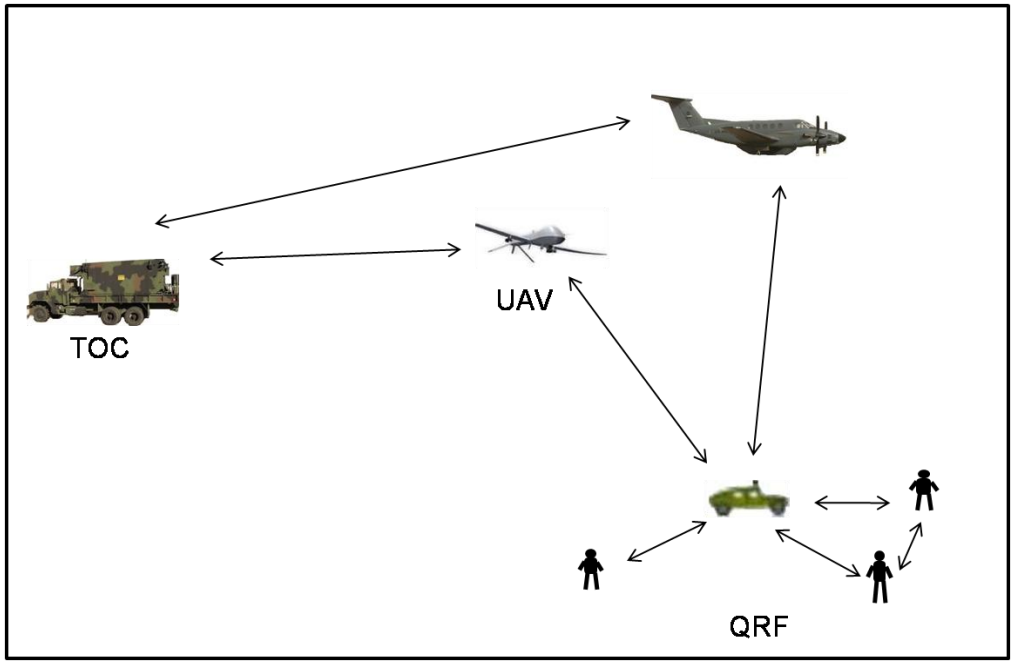

Figure 30. TNT ODIN Network

As shown in Figure 31 during the experiment, Simple Network Management Protocol (SNMP) is used to manage the network. Three CENETIX applications, Google Earth Situational Awareness (SA) Tool, VC1, which is a kind of collaboration tool, and Observer's Notepad are used respectively to measure the distance between units, communicate with the mobile unit, which represents QRF in the experiment scenario, and take note of significant actions and observed issues during the experiment.

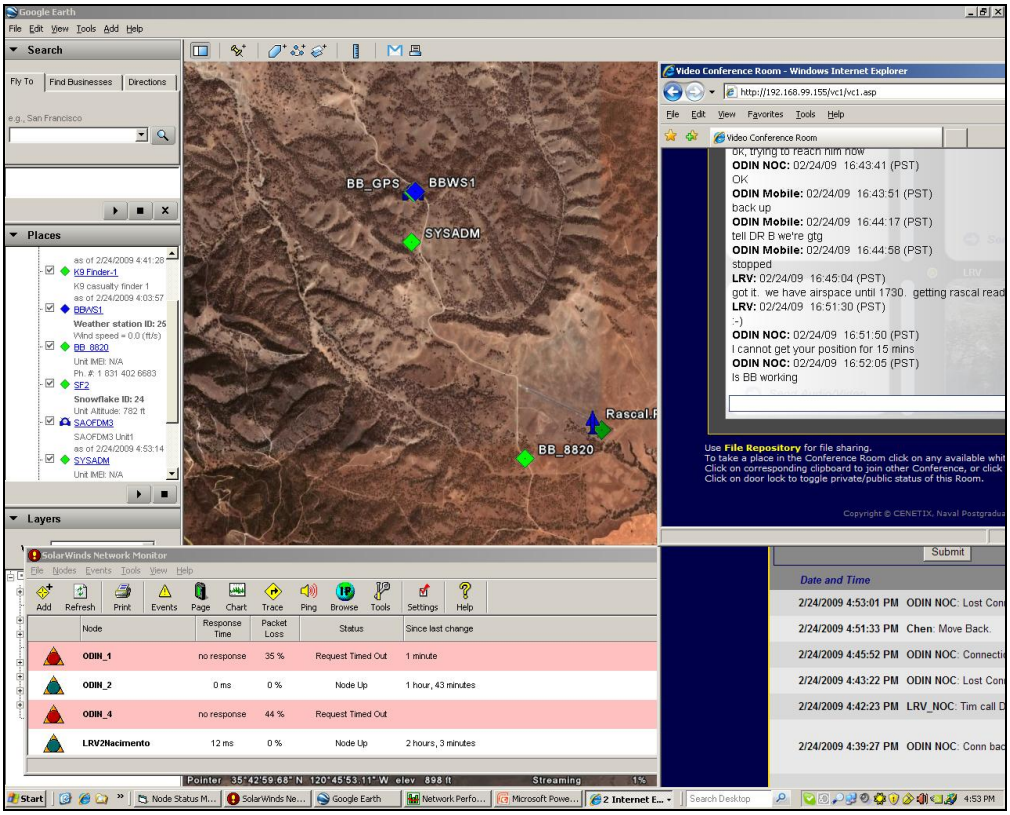

Figure 31. TNT ODIN Experiment Applications

Significant takeaways from the experiment—which are also very likely to happen on the war field—are discussed in the following paragraphs.

Interoperability of a different type or brand of radios is an important issue that should be considered every time. Even though all of the equipment is IP based, some interface problems can be experienced. In one of the experiments, the connection of IP based camera to Marine mesh radio fails since the radio's Ethernet port is not adaptive and the connection requires crossover cable.

Another important issue that must be considered is the flight pattern of the aerial relay. It is not possible to keep the aerial relay close to QRF every time. There are several factors that may force the aerial relay to lose line of sight to QRF. Distance from TOC and ground threat are two of such factors. As the relay moves out of the line of sight, the connection deteriorates and then is terminated.

As shown in Figure 32, as the distance between the mobile unit (shown as MOB) and the manned aircraft (shown as Jet) increases, communication becomes intermediate. In the experiment, this distance is measured at about 10 km. However, it is subject to many variables, such as weather, the aircraft's altitude, antenna type, transmitter power, receiver sensitivity, and terrain. Hence, in another scenario, it might be more or less than measured distance.

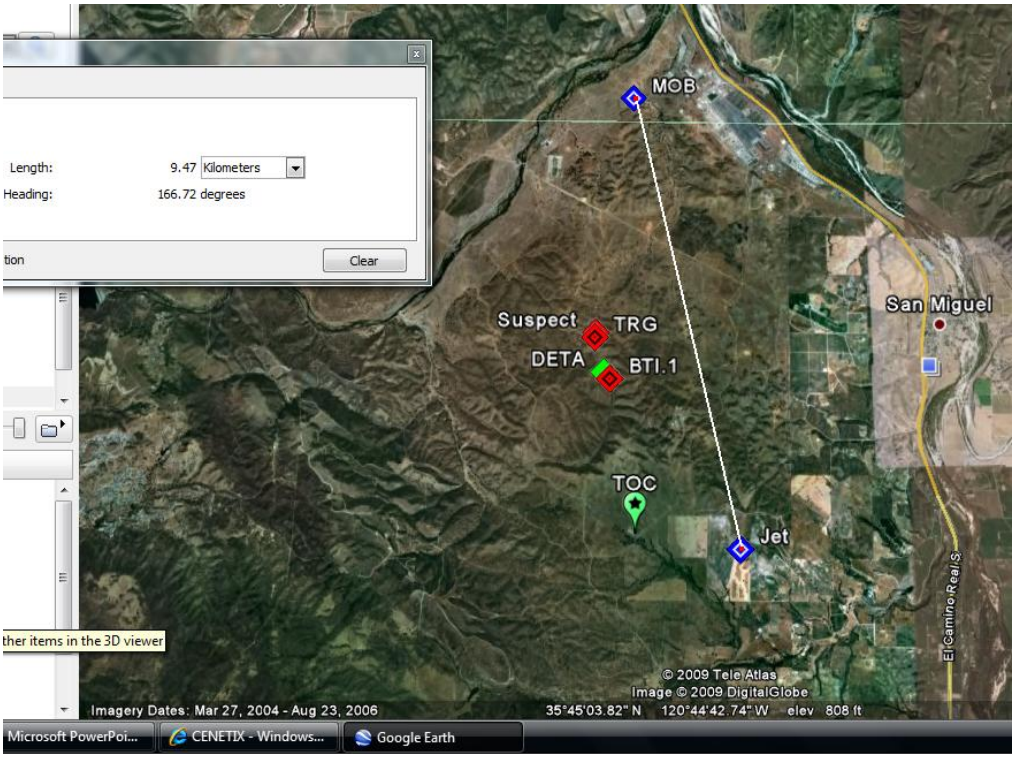

Figure 32. Maximum Communication Distance

In addition, in the same scenario, communication is lost when the manned aircraft gets very close to the mobile unit. As seen in Figure 33, when the manned aircraft gets closer to mobile unit, at about a 2–3 km distance, the connection deteriorates and is then lost. This is an unexpected situation and does not make sense at first. However, in after-action analysis; it turns out to be an antenna problem. The type of antenna on the manned aircraft creates a dead-zone under aircraft that prevents communication while it is flying over a mobile unit.

Figure 33. Locations of Units as Link Goes Down

The TNT ODIN experiment also tested the capacity of ad hoc networks established with hand held radios within a mobile unit. Tested mesh radios provide video streaming and allow control of an IP based camera connected to the radio from about 1 km distance within line of sight. Figure 34 shows the screenshot of video streaming sent from a user in a mobile unit to the TOC.

Although mesh radios provide video streaming from a distance, which is good enough for tactical units, the network only allows users to send data from one user to another user, i.e., network cannot provide multiple video stream transfers at the same time. In order to improve situational awareness throughout the ODIN Task Force, every unit or at least team leaders need to get and send data, which means more bandwidth.

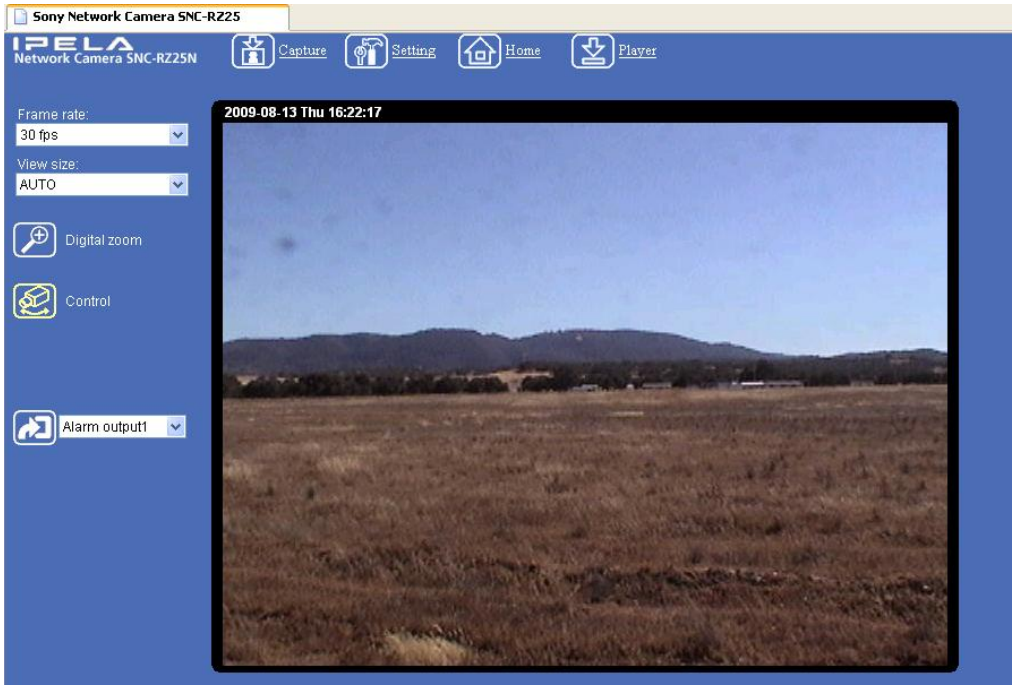

Figure 34. Mobile Unit Video Stream

The overall lesson learned from these experiments is that even with aerial relays, it is difficult to provide permanent communication in an ODIN scenario. Deploying more aerial vehicles might be suggested as a solution; however, this is not feasible every time and everywhere. Another solution is to implement a more efficient and adaptive network that will send more data when a link is available and/or automatically switch to other means of communication when a link is down. Since the bandwidth of alternative means of communication, like satellite, are not adequate to send all data, the suggested network should allow users to send critical information such as coordinates and information about any captured IED.

D. CBMANET IMPLEMENTATION

Although the CBMANET program will not have ended by the time this paper is written, results of first phase and demonstration show that it will significantly increase the efficiency of MANETs. This increased efficiency can be utilized in ODIN Task Force operations as a force multiplier.

CBMANET enables us to use the frequency spectrum more efficiently. In other words, it allows for the transmission of more data compared to currently used protocols. This lets QRF send/receive more data to/from TOC through an aerial relay while the link is up. It may also enable multicast distribution of data in the MANET, so that more fighters in the QRF share the information provided by TOC/ARST or other network users.

As shown in Figure 35, CBMANET enables QRFs, which are simultaneously conducting an operation, to keep coordinated, to be aware of each other, and to share information even when they do not have direct connection to the TOC. QRFs can communicate with each other through aerial relays or directly when they are in line of sight.

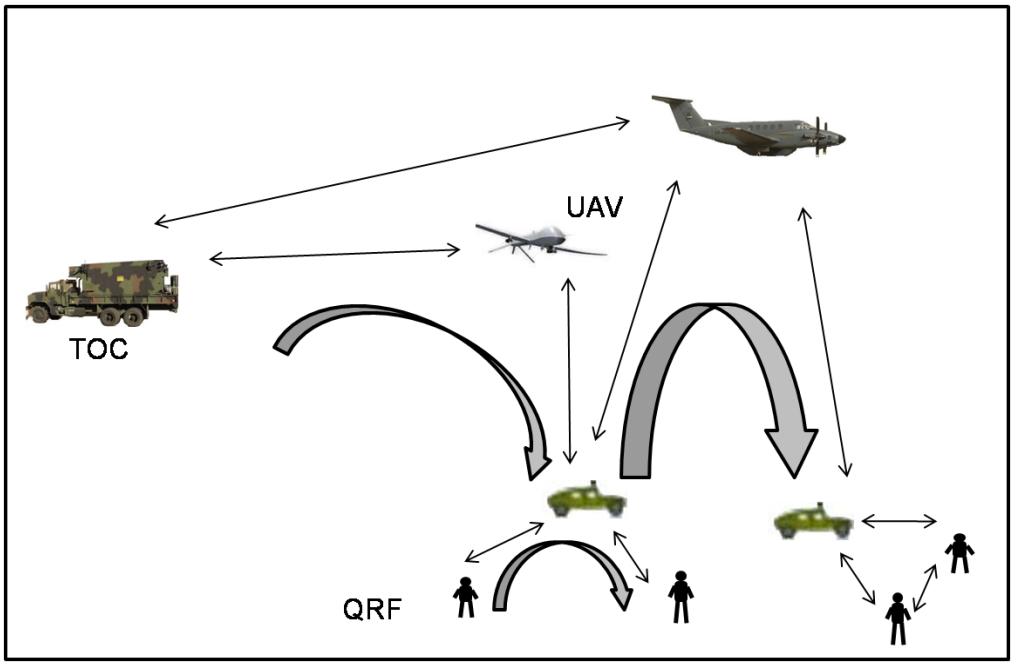

Figure 35. CBMANET Implemented ODIN Network

CBMANET provides an infrastructure to implement hyper-nodes or a kind of control system that will intelligently manage the MANET by utilizing the efficiency of network and adapting the network to continuously changing variables.

In addition to all aforementioned benefits, CBMANET can be easily implemented to networks that are equipped with SDRs. However, its interoperability with legacy system radios is questionable.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND SUGGESTIONS FOR FUTURE RESEARCH

Technology evolution and environmental effects drive behavioral changes in everyday life, as well as in a combat environment. Conventional wars are becoming a thing of the past. The characteristics of modern warfare are high tempo, short duration, continuous change of environment, and remote deployment. One key hallmark of warfare has remained constant over the ages; information is of the utmost importance and a key requirement for command and control. In fact, it might be safe to argue that accessing more and relevant information today whenever and wherever required is critical. The one who achieves information superiority gains a great advantage against his adversaries.

When high tempo operations are considered, MANETs stand out as the most convenient type of network, since individual nodes themselves provide the required infrastructure to establish the network. Accessing large amounts of accurate data in a very short time requires adaptive and efficient networks. It is at this point that questions about MANET capabilities arise. MANETs inherently have overhead in their network traffic for control purposes. This overhead reduces the efficiency of network. Because the resource, i.e., the frequency spectrum that MANETs use is scarce, low efficiency becomes an important problem that needs to be solved as demand for more and faster data increases exponentially.

The need for more data in a shorter period translates into the need for more available bandwidth and a reduction in latency. Seeking to provide more bandwidth and faster communication has prompted numerous organizations to initiate a myriad of studies, some of which are still going on today. New routing protocols have been introduced over the years. New types of antennas have been designed, and new modulation techniques have been developed. All of these continuous studies aim to increase the capabilities of each layer of the OSI

model. Although some of them are very successful, it seems to be that these studies will not be able to satisfy demands of MANET users in the future.

CBMANET, DARPA's revolutionary program, aims to provide the necessary efficiency for MANET users. CBMANET, with its optimized algorithms, decreases the overhead on the network traffic, which results in a reduction in latency and more available bandwidth. With this increased efficiency, it allows more data to be transferred to its users. CBMANET provides the infrastructure to implement hyper-nodes that can manage ad-hoc network intelligently, thus, MANETs become very adaptive and are successful in changing environments. In a tactical environment, more information that is provided more quickly by CBMANETs should definitely increase the success ratio and decrease incidents of friendly fire casualties. More information reduces one of the biggest threats for the combatant commander on the battlefield—the threat of uncertainty.

Uncertainty is surely something the special operations forces can do without in their missions. The Special Operations Forces (SOF) have arguably one of the hardest and most unique mission requirements on the planet. The current challenges of today, as well as challenges yet to be identified, will demand our best. Therefore, it is crucial that with the ever-changing political climate, as well as the rapid advancement of new technologies, that we do all we can to ensure that the SOF are always ready.

CBMANET can play a significant role in helping the SOF meet these challenges. The increased bandwidth and improved efficiency that CBMANET brings will increase the mobility, operational effectiveness, and global reach of the SOF. This increase will improve the quality of the data being passed from the SOF to its higher headquarters. The proposed improved quality will give the combatant commander better eyes on a potential target, or in certain scenarios like hostage rescues, better live-video feeds of the operation.

The increase will inherently bring with it very large data files that, in times past, had the potential to bring a network to its knees. CBMANET networks will

be the answer to this problem. In a study conducted by DARPA, they found that CBMANET improved performance by approximately seven times over the baseline [40]. DARPA further found in their studies that CBMANET consistently generated 2-3 times less traffic while providing better performance [40]. Everyone would have to agree that this is a very significant leap in performance improvement.

CBMANETs will not only benefit the combatant commander, but also all soldiers involved in the mission. The improved efficiency that CBMANETs possess will provide the special operations soldier with a greatly enhanced situational awareness on the battlefield. With this common operating picture, they will almost instantaneously know what friendly forces are in their area of operation and be able to monitor the actions of those forces. Everyone will be watching everyone. You could consider this as having the ultimate “big brother.”

CBMANET, as a technology, is still in its early stages and presents several areas for future research. Witnessing how well CBMANET performed in wooded terrain makes the average person wonder how it would perform if the terrain were different. There is no way of knowing where the next hotspot will be. Therefore, studies should be conducted in all types of climates using various scenarios in order to evaluate its impact more carefully. In addition, studies should be conducted to evaluate the effectiveness of its technologies with all types of software-defined radios, as well as all types of standard communications equipment used by conventional forces.

Since the terrorist attacks on 9/11, all service's missions have changed, specifically the Navy. Naval vessels are now more prone to conducting maritime interdiction operations or MIOs. These missions involve the boarding of possible hostile vessels in an effort to search for potential contraband. Most vessels are made of solid steel and can sometimes have several stories or decks. The boarding parties are required to transmit time-sensitive data to the base ship. CBMANET has to be proven to work efficiently in this type environment.

Finally, collaboration has become an essential part of this world's way of life. When pondering services like Facebook, Twitter, MySpace, and Youtube, it is easy to conclude that we, as a generation, love having information readily available to us. At any given time of the day we can pick up the technological device of our choice and instantly become situationally aware of the world in which we live in. Although CBMANET has the ability to dramatically improve the common operational picture on the battlefield, studies need to be conducted to determine those applications that works best with the technology.

LIST OF REFERENCES

[1] Merriam-Webster's Collegiate Dictionary, 11th Ed. Springfield, Massachusetts, 2003, p.15.

[2] M.S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations" in *IETF Network Working Group Request for Comments: 2501*, January 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2501.txt. [Accessed: April 7, 2009].

[3] J. Jubin and J.D. Tornow, "The DARPA packet radio network protocols," in *Proceedings of the IEEE*, January 1987, vol. 75, no. 1, pp. 21-32. [Online]. Available: IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 9, 2009].

[4] D.A. Beyer, "Accomplishments of the DARPA SURAN program," in *Military Communications Conference Record, A New Era*, 1990, vol. 2, pp. 855-862. [Online]. Available: IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 9, 2009].

[5] Advanced Network Technologies Division: Wireless Ad Hoc Sensor Networks. [Online]. Available: National Institute of Standards and Technology (NIST), http://www.antd.nist.gov/wahn_ssn.shtml. [Accessed: April 12, 2009].

[6] A. Bordetsky and R. Hayes-Roth, "Extending the OSI model for wireless battlefield networks: A design approach to the 8th Layer for tactical hyper-nodes," *International Journal of Mobile Network Design and Innovation 2007*, vol. 2, no. 2, pp. 81-91.

[7] A. Lazarus, "Information Theory for Mobile Ad Hoc Networks (ITMANET): Mission." [Online]. Available: http://www.darpa.mil/ipto/programs/itmanet/itmanet.asp. [Accessed: March 5, 2009].

[8] "ITMANET Solicitation," 2006. [Online]. Available: www.darpa.mil/ipto/solicit/baa/RFI-06-17.pdf. [Accessed: March 2, 2009].

[9] J.C. Ramming, "Information Theory for Mobile Ad-Hoc Networks (ITMANET): A fundamental studies program in the science of interconnected systems," March 2006. [Online]. Available: www.darpa.mil/ipto/programs/itmanet/docs/ITMANET_Presentation.pdf. [Accessed: March 2, 2009].

[10] R. North, N. Browne and L. Schiavone, “Joint Tactical Radio Systems: connecting the GIG to the Tactical Edge,” *MILCOM 2006 Military Communications Conference*, October 23–25, 2006, pp. 1–6. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: March 2, 2009].

[11] J. Mitola, III, “SDR architecture refinement for JTRS,” *MILCOM 2000 21st Century Military Communications Conference Proceedings*, 2000, vol. 1, pp. 214–218. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: March 22, 2009].

[12] A. Feickert, “The Joint Tactical Radio System (JTRS) and the army’s Future Combat System (FCS): Issues for Congress,” November 17, 2005. [Online]. Available: http://digital.library.unt.edu/govdocs/crs//data/2005/upl-meta-crs-7941/RL33161_2005. [Accessed: March 25, 2009].

[13] “Joint radio system programmable, modular communications system.” [Online]. Available: www.globalsecurity.org/military/systems/ground/jtrs.htm. [Accessed: March 25, 2009].

[14] M. Craven, T.N. Le and P.Lardieri, “DVoIP: Dynamic voice-over-IP transformations for quality of service in bandwidth constrained environments,” in *Military Communications Conference*, 2008, pp. 1–6. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: March 30, 2009].

[15] P. Lardieri and D. Dacosta, “Synthesizing adaptive protocols by selective enumeration (SYNAPSE),” guest lecturer notes for IS4926, Department of Information Systems and Technology, Naval Postgraduate School, Winter 2009.

[16] C. Ogut, “An ad hoc wireless mobile communications model for Special Operations Forces,” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2000.

[17] L.K. Thong, “Performance analysis of mobile ad hoc networking routing protocols,” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2004.

[18] M. Halvardsson and P.Lindberg, “Reliable group communication in a military mobile ad hoc network,” A report from School of Mathematics and Systems Engineering, Vaxjo University, Sweden, February 2004. [Online]. Avaliable: http://vxu.se/msi/utb/exarb/2004/04006.pdf. [Accessed: March 31, 2009].

[19] J. Doshi and P. Kilambi, “SAFAR: An adaptive bandwidth-efficient routing protocol for mobile ad hoc networks,” in *Ad-Hoc, Mobile, and Wireless Networks: Second International Conference, ADHOC-NOW 2003 Montreal, Canada, October 2003 Proceedings*, S. Pierre, M. Barbeau and E. Kranakis Ed. Berlin: Springer 2003, pp.12–24.

[20] G.L. Pore, “A performance analysis of routing protocols for ad hoc networks,” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2006.

[21] G. Kioumourtzis, “Simulation and evaluation of routing protocols for mobile ad hoc networks (MANETs),” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2005.

[22] I. Shin and C. Lee, “Enhanced power-aware routing protocol for mobile ad hoc networks,” in *Ad-Hoc, Mobile, and Wireless Networks: 4th International Conference, ADHOC-NOW 2005 Cancun, Mexico, October 2005 Proceedings*, V.R. Syrotiuk and E. Chávez Ed. Berlin: Springer 2005, pp. 285–296.

[23] R. Menchaca-Mendez, R. Vaishampayan, J.J.Garcia-Luna-Aceves and K. Obraczka, “DPUMA: A highly efficient multicast routing protocol for mobile ad hoc networks,” in *Ad-Hoc, Mobile, and Wireless Networks: 4th International Conference, ADHOC-NOW 2005 Cancun, Mexico, October 2005 Proceedings*, V.R. Syrotiuk and E. Chávez Ed. Berlin: Springer 2005, pp.178–191.

[24] M.S. Gast, *802.11® Wireless Networks: The Definitive Guide*, 2nd Ed. Sebastopol, CA: O’Reilly, April 2005, pp. 311–342.

[25] T.K.Paul and T. Ogunfunmi, “Wireless LAN comes of age: understanding the IEEE 802.11n Amendment,” in *Circuits and Systems Magazine*, IEEE, 2008, vol. 8, no. 1, pp. 28–54. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 4, 2009].

[26] T. Carpenter and J. Barrrett, Ed., *Certified Wireless Network Administrator Official Study Guide*, 4th Ed. New York: McGraw-Hill, 2008.

[27] G. Goth, “New Wi-Fi technology racing past standards process,” in *Distriburted Systems Online, IEEE*, Oct. 2008, vol. 9, no. 10, p. 1–1. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 4, 2009].

[28] A. Goldsmith, S.A. Jafar, N. Jindal and S.Vishwanath, “Capacity limits of MIMO channels,” in *Selected Areas in Communication*, IEEE, June 2003, vol. 21, no. 5, pp. 684–702. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 4, 2009].

[29] R. Olexa, *Implementing 802.11, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations*, Burlington, MA: Elsevier, 2005, pp. 14–17.

[30] A.S. Patrick, “An analysis of IEEE 802.16 and WIMAX multicast delivery,” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2007.

[31] A. Bordetsky and E. Bourakov, “Adaptive-on-demand networking with self-aligning wireless nodes,” A report from Center for Network Innovation and Experimentation (CENETIX), Naval Postgraduate School, Monterey, CA, 2006. [Online]. Available: http://cenetix.nps.edu/cenetix/documents/SAOFDM%202006.doc. [Accessed: April 4, 2009].

[32] Lawrence Livermore National Laboratory, “Engineering at LLNL: UWB communication,” *Lawrence Livermore National Laboratory*, UCRL-WEB-215972, November 18, 2008. [Online]. Available: https://www-eng.llnl.gov/uwb_comm/uwb_comm.html. [Accessed: April 7, 2009].

[33] J. Foerster, E. Green, S. Somayazulu and D. Leeper, ”Ultra-wideband technology for short- or medium-range wireless communications,” in *Intel Technology Journal: Networking and Communications*, May 2001, vol. 5, no.2. [Online]. Available: Intel, http://www.intel.com. [Accessed: April 7, 2009].

[34] S.M. Mirhosseini and F. Torgheh, “Improvement of TCP performance in ad hoc networks using Cross layer approach,” in *ICSNC’08 3rd International Conference: Systems and Networks Communications*, October 2008, pp. 322–328. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 10, 2009].

[35] N. Young, R. Sankar and J. Lee, “Improving ad hoc network performance using cross-layer information processing,” in *IEEE International Conference: Communications*, May 2005, vol. 4, pp. 2764–2768. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 10, 2009].

[36] W.H. Yuen, H. Lee and T.D. Andersen, “A simple and effective cross layer networking system for ad hoc networks,” in *The 13th IEEE International Symposium: Personal, Indoor and Mobile Radio Communications*, Sep. 2002, vol. 4, pp. 1952–1956. [Online]. Available:IEEE Xplore, http://ieeexplore.ieee.org. [Accessed: April 10, 2009].

[37] A. Goldsmith, et al., “Cross-layer design of ad hoc wireless networks for real-time media,” A project from Stanford University, USA, June 2008. [Online]. Avaliable: http://www.stanford.edu/~zhuxq/adhoc_project/adhoc_project.html. [Accessed: March 31, 2009].

[38] J.C. Ramming, “Promising Approaches to Clean-slate Wireless Networking,” in Stanford Clean-slate Networking Seminar, April 24, 2008. [Online]. Available: http://netseminar.stanford.edu/seminars/04_24_08.pdf. [Accessed: January 19, 2009].

[39] D.S. Alberts, J.J. Gartska and F.P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication, 1999.

[40] G. Lauer, “CBMANET Phase 2 Demonstration,” CBMANET Demonstration Briefing Slides, July 31, 2009, Hayes Field Columbia, MD.

[41] “DARPA Awards BAE Systems Wireless Tactical Network Contract.” [Online]. Available: http://www.insidedefense.com/secure/display.asp?docnum=dplus2006_2107&f=defense_2002.ask. [Accessed: July 23, 2009].

[42] “The Control-Based Mobile Ad-Hoc Networking (CBMANET).” [Online]. Available: http://www.darpa.mil/sto/strategic/cbmanet.html. [Accessed: July 14, 2009].

[43] J.C. Ramming, “Control Based Mobile Ad-Hoc Networking (CBMANET) Program Motivation & Overview,” August 30, 2005. [Online]. Available: http://www.darpa.mil/sto/solicitations/cbmanet/briefs/CBMANET_Overview-Ramming.pdf. [Accessed: November 11, 2008].

[44] FY 2009 Budget Estimates, “RDT&E Budget Item Justification Sheet,” Available: http://www.dtic.mil/descriptivesum/Y2009/DARPA/0602303E.pdf. [Accessed: August 8, 2009].

[45] G. Lauer and V. Marano, “Field Experiment 6 VIP Demonstration Plan,” CBMANET Demonstration Briefing Slides, July 31, 2009, Hayes Field Columbia, MD.

[46] Joint Publication 3-05, Doctrine for Joint Special Operations, 17 December 2003

[47] A. Toffler and H. Toffler, *War and Anti-War: Survival At the Dawn of the 21st Century*, Boston: Little, Brown, 1993.

[48] United Sates Special Operations Forces Posture Statement: Transferring the Force at the Forefront of the War on Terrorism, 2003–2004.

[49] USSOCOM C4I Strategy into the 21st Century, MacDill AFB, FL: U.S. Special Operations Command, 1996.

[50] "Task Force ODIN," November 11, 2008. [Online]. Available: http://www.globalsecurity.org/military/agency/army/tf-odin.htm. [Accessed: July 27, 2009].

[51] A.T. Ball and B.T. McCutchen, "Task Force ODIN Using Innovative Technology to Support Ground Forces," September 20, 2007. [Online]. Available: http://www.blackanthem.com/News/Military_News_1/Task_Force_ODIN_Using_innovative_technology_to_support_ground_forces10239.shtml. [Accessed: July 27, 2009].

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Savunma Bilimleri Enstitusu
   Kara Harp Okulu, Bakanliklar, 06100
   Ankara, Turkey

4. Dan Boger
   Naval Postgraduate School
   Monterey. California

5. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

6. Michael Clement
   Naval Postgraduate School
   Monterey, California

7. Mustafa Masacioglu
   Genelkurmay Bilgi Sistemler Daire Baskanligi, Bakanliklar, 06100
   Ankara, Turkey

8. Marlon McBride
   Naval Postgraduate School
   Monterey, California